SELECTION OF JPEG STEGANOGRAPHY ALGORITHMS USING A FEATURE BASED MODEL

Vijayanathan Senthooran

(128005D)

Degree of Master of Philosophy

Department of Information Technology

University of Moratuwa
Sri Lanka

November 2018

SELECTION OF JPEG STEGANOGRAPHY ALGORITHMS USING A FEATURE BASED MODEL

Vijayanathan Senthooran

(128005D)

Thesis is submitted in partial fulfillment of the requirements for the degree Master of Philosophy

Department of Information Technology

University of Moratuwa
Sri Lanka

November 2018

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: Date:

The above candidate has carried out research for the MPhil thesis under my supervision.

Name of the Supervisor: Dr. Lochandaka Ranathunga

Signature of the Supervisor: Date:

ACKNOWLEDGEMENT

Firstly, I am indebted to my supervisor Dr. Lochandaka Ranathunga for his kind cooperation, guidance, and supervision extended throughout this research project. Without his insight, this work would not be possible. I would like to express my heartfelt thanks to the Vice Chancellor of the University of Moratuwa, the Dean of the Faculty of Information Technology and the Head of the Department of Information Technology, University of Moratuwa for granting me the opportunity to commence my research work at the University of Moratuwa and facilitating me to carry out same successfully. Further, I would be failing in my duty if I do not extend my sincere gratefulness to the Rector of the Vavuniya Campus of the University of Jaffna, the Dean of the Faculty of Applied Science and the Head of the Department of Physical Science, Vavuniya Campus of the University of Jaffna for granting me two years paid study leave and releasing me from all academic duties in the Campus, thus allowing me to concentrate fully on my research work during the said two years. Thanks are also due to the Director and staff of the National Science Foundation, Sri Lanka for granting a research scholarship under the grant number NSF/SCH/2013/04 to financially support this effort.

I would like to thank all the staff members of the University of Moratuwa for their cooperation and commitment extended in various ways in order to make this project a success. The support and motivation provided by my post graduate friends, Mr. A.M.R.R. Bandara, Mr. Saneera Hemantha Kulathilake and Mrs. N.M. Wagarachchi at the Faculty of Information Technology, University of Moratuwa too deserve mentioning with a debt of gratitude.

I would like to express my appreciation to Mr. T. Kartheeswaran for his immense support and contribution to make this thesis a success. Last but not least, I offer a debt of gratitude to my parents, my wife, my son and my brothers for all their encouragement and support extended right through this endeavor. Finally, I am grateful to all those who assisted me in numerous ways during the course of this research.

Abstract

JPEG image steganographic techniques use the DCT coefficients scaled by quantization table to make secure data hiding without degrading the image quality. The selection process of data embedding locations in lower frequency DCT coefficients should be carefully considered in each image blocks as these lower frequency coefficients are high sensitive to human eyes. Some of the existing related JPEG steganographic methods have been proposed with primary quantization table modification to hide message bits in the quantized DCT coefficients with minimal distortion by analyzing the properties of quantization table entry and relevant DCT coefficients. The performance of the JPEG steganographic methods is evaluated by the imperceptibility and embedding capacity. In the literature of quantization table modification based JPEG steganography, the middle frequency coefficients in each image block are utilized to embed maximum message size by modifying the middle part of the relevant quantization table values with minimizing the effect of visual perception. However, the data hiding techniques in lower frequency coefficients from the existing studies endure from imperceptibility while increasing the message size. This study suggests the lower frequency data hiding algorithms with utilizing middle frequency data hiding in terms of the modification of lower and middle part of the quantization table values by evaluating image quality parameters and it doesn’t affect the perceptual detectability and improves embedding capacity. The proposed JPEG steganography investigates the modification of quantization table values with regarding to selected lower frequency DCT coefficients for data hiding and selects different data hiding patterns in lower frequency area in terms of modification of quantization table. Finally, it returns the pair of relevant modified quantization table and generated data hiding pattern for an image based on the empirical results of the PSNR values. The pair that contains modified quantization table and data hiding pattern shared by the sender is used as a secrete key to extract the message at the receiver side. From the preliminary studies, the selection of appropriate lower frequency coefficients in image block to hide the optimum size of secrete message with perceptual un-detectability is dependent on the combination of image features, message size and the hiding algorithm. Further, this study recommends a dynamic model to keep the consistency of the combination of image features, message size and the hiding algorithm in terms of quantization table modification and this model based steganography suggests a dynamic model to cover image statistics. Eventually, the model prevents visually perceptible changes for maximum embedding message bits. The proposed method achieves a good imperceptibility level and it is evaluated by the PSNR value range 30dB to 45dB and maximum message size more than 52 bits per block for the selected JPEG image dataset. The dynamic model fitted between the quantization tables and cover image statistics shows the statistical significance with the p-value 0.0007634 and the model generated between the data hiding pattern and statistical features of DCT coefficients shows the statistical significance with the p-value 4.598e-13. The dynamic model for the selected data hiding patterns in the lower frequency coefficients hides the message and it is stego invariant for message analyzers.

Key words: JPEG Steganography, imperceptibility, embedding capacity, quantization table, DCT transformation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1
INTRODUCTION

In the digital era of information communication technologies, the revolution of digital information brings major changes to our community and daily routine activities. Internet and other types of networks provide secure channels to transfer digital information. Consequently, the open information transmission over these channels is secured by encryption techniques to prevent the secrete message content from adversaries on cyber space. The rapid growth of technological aspects of information security, the users on cyber space without having the knowledge of encrypted message will depict redundant attention to data hackers. This will lead that the encrypted message appeared as a string of gabble data might intend notion of the encrypted message. In addition, the possibility of illicit operation by interested hackers may attempt to the liability of encrypted message. Thus, the encrypted secrete message could be illegitimately interrupted and hacked during the data transferring process [1]. In order to solve the problem of the vulnerability of encrypted message during the data transmission, the process of steganography is established as another approach to hide secrete message into innocent digital media in order that the secrete message can be transmitted silently over the open communication channels without detecting any avoidable attention of data hackers. In few words, steganography is the discipline of hiding secretes information by an assured procedure of embedding a digital object into another digital object [2]. The concept of steganography generates from the idea that the secrete message hidden inside the digital object should not be perceptible to Human Visual System (HVS). Thus, two important considerations of steganography are imperceptibility and secrete message capacity (embedding capacity). The more information embedded into the carrier, the noise will be increased in the carrier. This yields a tradeoff between the imperceptibility and embedding capacity. The performance of steganography is evaluated by perceptual quality factors and volume of hidden message. The primary objective of any steganographic system is to hide maximum amount of secret message bits inside the carrier without perceptual transparency of carrier that satisfies the security concern with the ability of disclose [3].

1.1 Information Security and Steganography

Due to the huge propagation of multimedia contents over the Internet and World Wide Web (WWW), the multimedia contents are used as transmission medium to carry the message from sender to receiver because of the redundancy of the visibility of multimedia contents [4]. Because of digital transactions, security concerns, at that time, the preference will be enabled to receiver who has the capability to interpret the hidden information contents transferred through communication. Although, the significance of secret communication can be secured by encryption technique, the complete communication process is obvious to data hackers in the encryption technique. Hence, the communication between sender and receiver should be kept on secret manner. Data hiding is the solution to keep the communication on secret manner. Data hiding occupies hiding considerable secrete information into a variety of digital media such as text, image, audio and video. The usage of data hiding has been widely accepted in the application of copyright protection, fingerprinting and other secret communication [5]. The principle of data hiding techniques in digital content is varying from that of cryptography or watermarking techniques. Secrete messages are encrypted into meaningless data in cryptographic algorithms while copyright matters are protected in watermarking algorithms. Data hiding algorithms wraps the secret message with the cover media as mask and is considered as an expansion of traditional cryptography [6].

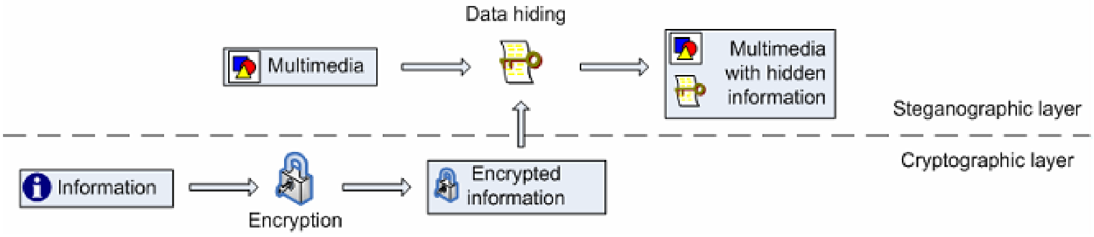


Figure 1.1: The principal difference between the function of cryptography and steganography [1].

Figure 1.1 shows the sketch of steganography and the significant difference between cryptography and steganography are differentiated based on their functionality. Steganography is the ability of embedding information secretly into multimedia content such as text, image, audio and video. Secret messages can be embedded inside the digital contents such as text, images, and audio, video and network protocols. These digital contents are named as cover medium and the resultant of the cover medium attached with message to conceal is termed as stego file [3]. The major concern of a cover medium is the data embedding capacity inside the cover file without being detectable by an adversary. When the quality of a cover file is degraded, message analyzers will suspect and try to check strictly. The stego file can be easily hacked and propagated over the internet. Modern Steganographic techniques are intended to develop fashionable styles of information replacement. In steganographic techniques, it is observed that the embedding capacity limits for the secrete message are determined by the data-embedding techniques [7]. Therefore, it is important to exploit the embedding capacity, present reversible data recovery and provide flexibility to retrieve the secrete message bits even as hiding the presence of the hidden information from the adversary.

The major objective of steganography is to conceal secrete information inside the cover media in order that a third party will not become aware of the existence of the secret information. In this way, steganography shows the major feature between others of secret exchange of information, for an example, especially in cryptography, a third party observes the secret information by considering the encoded information suspiciousness but they will not be capable to understand the secret information. On the other hand, steganography enables the existence of the secret information in the cover media which will not be perceived at all.

In information security, cryptography and information hiding achieves separate goals. Cryptography covers only the contents of secret information from an adversary, but steganography cover the presence of secrete information. Thus, steganography gives more privacy and security of secrete information than cryptography as it hides the survival of secrete information rather than shielding the message contents. The drawback of cryptography is the visibility of encrypted message to third parties. It only protects the message but the existence of message is open to all. In terms of failure or breaking of secure data transmission system over communication channels, both steganography and cryptography are treated in different manner. A cryptographic method is considered as fail or breaking by hackers if an adversary can be able to read the encrypted secrete message. However, a steganographic system is considered as breaking if an adversary can be able to notice the presence of the secrete message or read the secrete message inside the cover medium [2]. Furthermore, the primary concern of any steganographic system failure is the perceptual or statistical suspicion of steganographic system by attackers (or steg-analyzers) without considering the knowledge of hiding pattern of secrete message. Therefore, steganographic system is considered more possibilities for breakable compared with cryptography according system failure. Eventually, a steganography system is deemed as secure system if it must keep away from any kind of destruction from attackers. From the above-mentioned aspects of both steganography and cryptography, in ultimate secure data transmission system, steganography complements cryptography to avoid increase the suspicion level of third parties. Steganography provides extra layer of data transmission security over the communication channels [9]. The suspicion of the existence of encrypted message, employed data hiding pattern and encryption algorithm inside the cover medium are the three challenges for attackers. Presently, the combination of steganography and cryptography used with compression attains about to ideal secure solution for information security [1]. Two another information hiding techniques intimately connected to steganography are fingerprinting and watermarking which are mainly related with the safeguard of intellectual property rights of digital media [9]. Watermarks protect digital media against exclusion of copyright information of digital media. The digital media exist with watermark is visible; it should be harder to remove the copyright of digital media from watermarked file exclusive of destroying or distorting the watermarked object. The feature of this functionality is known as robustness of watermarking. The robustness is the very important property of watermarking and it is significantly distinguishing watermarking from steganography. The main theme of steganography and watermarking is data hiding with some common characteristics. The aim of steganography is to conceal the existence of communication by hiding secrete message inside the cover objects. Conversely, the aim of watermarking is to protect the rights of the proprietor of digital media such as text, image, sound, video and software. The adversary or users on internet try to modify or duplicate the watermarked file, the owner of the watermarked file shows to prove of his or her originality of property [10]. Another kind of information hiding technique to protect the intellectual property rights of digital media is fingerprinting. The process of fingerprinting is to embed unique marks or serial number in every copy of the digital file (cover object) which are distributed to different customers [11]. The intention of fingerprinting process mentioned above is to enable the property owner of the digital file easily recognizes their clients who crack their license or key by providing the property to others. If the hidden mark or serial number is detected in the process of fingerprinting, it is impossible to remove it. The principle difference between these three information hiding techniques (steganography, watermarking and fingerprinting) is the object of communication. In watermarking and fingerprinting, the object of communication is carrier file with hidden data that provides copyright protection. In contrast, steganography uses embedded data as object of communication that means carrier object is used as cover file. The hidden information inside the digital content is visible or public knowledge in watermarking and fingerprinting techniques. However, in steganography, imperceptibility of the hidden information inside the cover file is very essential. While the breaking of watermarking or fingerprinting system is not to detect the hidden mark but to remove the hidden mark [12], the breaking of steganography system consists of the third parties suspect the existence of hidden information inside the carrier file.

1.2 Stenography and the ability of secrete communication

Steganography enables the ability of hiding secure communications between two parties over the harmless cover medium, in order that it cannot be suspected by internet hackers. In compare with encryption technique where the objective is to have secure communications from an Internet attacker, steganographic techniques attempt to hide the very existence of the secrete message itself from an attacker.

Steganography uses multimedia as a medium such as image, audio, or video to hide the secret information. The redundant bits in any medium are used to hide data and then it is named as cover medium. After embedding secrete message bits in any cover medium, thus a stego medium is attained. As a whole, a steganographic approach begins by searching redundant bits in a cover medium. Redundant bits can be used to modify without distorting the statistical features of the cover medium. A steganographic method utilizes these redundant bits for secrete message hiding without altering the statistical properties of the cover medium [13]. Modification of redundant bits enables to detect traces in most of the steganographic methods. Even if the embedded message is not showed, the presence of it is detected. The secrete message transmission deployed in a steganographic system is carried out in such a manner that an adversary cannot guess that there is a hidden content is changed over between sender and receiver except exchange of any type of media files. The strength of any steganographic approach is developed to use only the redundant bits to embed secrete message without degrading the cover media statistical properties. After hiding the secrete message bits in an innocent cover medium, the derived stego medium should be kept securely against statistical and visual attacks and robustness against vulnerability of stego medium [14] .

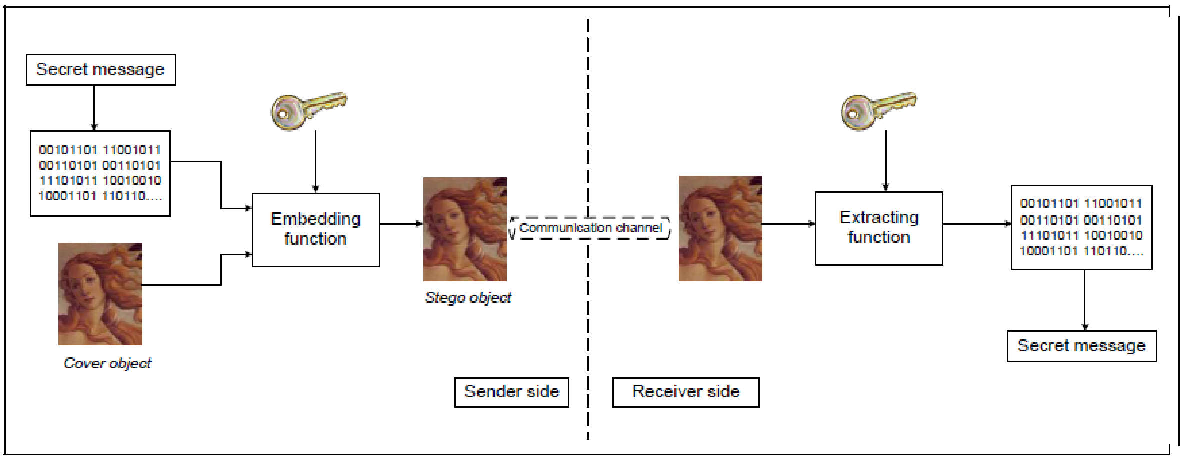


Figure 1.2: Illustration of steganography system [14].

1.3 Types of steganography based on its mechanism

1.3.1 Key based

Pure steganography

It is the type of steganography system which has no knowledge of prior replacement of secrete message before transmitting message. Therefore, no keys are used to start the steganography process. The efficiency of this steganography system is fully depending on the existence of communication inside the cover object [15].

Public key steganography

The public key steganography needs two keys, one is private key (secrete key), another one is public key and is not depend on the exchange of private key.

The sender uses the receivers public key to encrypt the secrete message and embeds inside the cover object known to receiver. The embedding process is public. The receiver who has no information about embedding algorithm will notice the arrival of message and simply try to retrieve and decrypt the message using his private key [15].

Secrete key steganography

The sender selects the cover and hides the secrete message inside the cover using a secrete key which is known to receiver. The receiver can do the reverse process to extract the secrete message using the same secrete key. No one who does know the secrete key used in this process should not be able to attain the existence of encoded information. This steganographic system obeys the Kerckhoff's theory [16] . Most of the researchers use this secrete key steganography system as the entire knowledge behind the stego object could incorporate the entire knowledge of cover object, it is too difficult for the third parties to obtain the secrete message.

1.3.2 Countermeasures against steganography

Passive warden scenario

The passive warden scenario observes the secrete communication without any obstruction. Hence, if the warden has restrictions to alter the ingredients of stego object during the data transmission process, it is entitled as a passive warden scenario which prevents or allows the message delivery [17]. Consequently, if the warden guess that a secret communication is happening, the data transmission process between sender and receiver will be blocked. Otherwise the communication will be continued. Presently, the most of the steganographic techniques reflects on passive warden scenario in which third parties does not impede the communication but just observe the communication. Our proposed approach is indented to reflect on the passive warden approach.

Active warden scenario

The active warden scenario deliberately alters the ingredients of stego object or files during the data transmission process. The process of active attack is the modification of the stego file to establish noises during the communication process so as to prevent secretes communication [17].

In this scenario, third parties can get and alter the stego file from the sender and then forward this altered stego file to receiver in order to destroy any secrete message inside the stego file. From the point of view of active warder scenario, it is the challenge to protect the secrete communication from the active attacks. It is one of the problem domains in steganographic techniques. On the other hand, steganography system that refuse to accept this type of attacks and protect the legibility of secrete message at the receiver side is called as robustness of the steganography system. This type of scenario is most probably to be employed for watermarking and fingerprinting techniques rather than steganographic techniques.

1.3.3. Embedding methodology based categorization

In spite of the cover file used for data embedding, insertion, substitution and generation techniques are the three broader categories of data embedding methods in steganography system [18] [19] [20]. Further, this type of steganography system is the most favored approach in the steganography research community.

Data insertion method

The data insertion methods embed secrete message in some area of a cover file which is ignore by some file processing applications and this method does not alter the significant area of a cover file related to the receiver. The size of the resultant file would be increased as this method hides secrete message in the part of a cover file. The benefit of this method is that the actual contents of cover file would not be modified in terms of data hiding [21].

Substitution method

In contrast to insertion method, the substitution method does not accumulate the secrete message to the cover file. It finds some trivial regions or information of cover files and utilize this regions to hide the secrete message. Substitution method substitute data bits from the cover file by data bits of secrete message. This method does not increase the size of the cover file. However, based on the statistical features of cover file and the functionality of embedding method, the substitution method may yield the result with regarding to degradation of cover file or object. Further, the payload capacity is restricted by the amount of trivial of information of cover files [22].

Generation method

In contrast to insertion and substitution methods, the generation method does not require a cover file ever since this method uses secrete message to relevant stego files. Among the steganography detection methods, one is to compare the originality of cover file with stego file. Here, the generation method takes the advantage of preventing such type of steganography detection method because of stego files are only used in this generation method to hide the data. That means no cover files used. The inadequacy of this method is that generation of stego files is limited and resultant stego file might be impractical to receiver. The main aspect of this generation method is to achieve the dependency between the features of cover objects and secrete message composition [23].

Besides the general information hiding methods briefly discussed above, abundant steganography techniques developed from the above information hiding methods have been used by the steganography research community. These techniques vary in terms of the principle of data hiding mechanism used in each method. Another six steganography techniques additionally identified by are substitution techniques, transform domain techniques, statistical method based techniques, spread spectrum techniques, distortion techniques and cover generation techniques to hide the secrete message inside the cover medium.

1.3.4 Carrier based categorization

There are many varieties of steganographic techniques available in digital medium in order to attain data security depending on the type of the cover medium. They are briefly described as follows.

Text Steganography:

Text steganography can be skilled by the modification of quality of textual contents in cover medium. The aim of the text steganography is to make alteration that is depend on embedding algorithm [24].

Image Steganography:

Digital images are the mostly used as well-known cover medium for steganography. In the digital image domain, a lot of different image file formats support for distinct applications and different steganographic algorithms. The image steganography techniques take advantage of the limitation of the human visual system (HVS). In simply, digital image steganography is a method of data embedding into cover-image and produces a stego-image then this stego-image is used to send to the receiver by well-known transmission medium, where the data hackers have a doubt that this generated resultant image with secrete message. After arrival of the stego-image at the receiver side, embedded secrete message can purely be retrieved by using key that depends on the data embedding technique [5]. In this extensive study, robustness, imperceptibility and embedding capacity enhancement of image steganography has been investigated.

Audio Steganography:

In audio steganography techniques, digitized sound signal is utilized to embed secrete message that yields minor changes relating to cover audio file. Audio steganography uses three main methods to encode the cover audio files. They are echo hiding, LSB and phase encoding method [25]. Audio steganography has turn into very important medium as a result of voice over IP (VOIP) reputation. Further, Audio steganography supports digital audio formats such as WAVE, MIDI, AVI, and MPEG. The benefit of audio steganography compared to other medium is sound frequency changes at every single bit. It entails more security of the steganography method.

Video steganography:

Video Steganographic techniques are used to hide secrete data into digital video files. The combination of digital images is used as cover medium for concealed information. In the main, discrete cosine transform (DCT) adjusts values that is utilized to embed the secrete data in each of the image frames in the video file. The generated video file is not visible by the HVS. Video steganographic techniques support different file formats, such as H.264, Mp4, MPEG, and AVI [26].

Network protocol steganography:

Protocol steganography embeds the information using network control protocol like http, ftp, tcp, Ssh, udp etc. Protocol steganography is an advance dimension of steganography and more secure than other dimensions. Many researchers are working on it to improve its technique so that it can be applied for hiding other forms of data on various protocols.

The Network Protocol Steganography can be attained with unemployed header bits of TCP/IP fields in covert channels that exist in the OSI network layer [27].

1.4. Steganography in digital images

1.4.1 Data hiding in digital images

Hiding data in digital images faces a variety of challenges that happen caused by the way of Human Visual System (HVS) works and the distinctive modifications made in images. Generally, digital images present a relatively little host signal for hiding data and they will be subject to variety of operations ranging from simple affine transforms to nonlinear transforms such as cropping, blurring, filtering, and lossy compression [28]. Convenient data-hiding techniques need to be challenging to as many of these types of transformations as possible. In spite of these challenges, still digital images are selected as best candidates for data hiding. Many attributes of the HVS are the important factors to utilize the efficiency of data hiding techniques. Data hiding in digital images entails embedding relatively large amount of secret information into a host image with negligible perceptible degradation of image quality [29]. However, the embedding capacity for secret information and the distortion of the host image are a trade off as more hidden secrete data results in more degradation on the visual appearance of the cover image for all time [30]. Furthermore, while data hiding is applied on the compressed images, the embedding capacity and the imperceptibility of cover images can be further controlled [31]. With the fast advancement of Internet technology, Internet users can be able to transmit and share digital objects with each other easily. In order to secure the efficiency of communication and keep network bandwidth consistently, compression techniques can be deployed on digital contents to diminish redundancy, and the quality of the decompressed digital content should also be conserved. These days, much more digital content, particularly digital images and videos, are transformed into the compressed domain for transmission. Another vital point in an open network environment is how to send out secret or private data in secure manner. Even if conventional cryptographic techniques encrypt the plaintext into the cipher text, the encrypted random data of the cipher text may also arouse the doubt from the third party [32]. To resolve this key issue, data hiding techniques have been broadly initiated in various applications such as academic, industry and military that employs data hiding into cover image unnoticeably. Due to the propagation of digital images on the Internet, compression algorithms on digital images and data hiding into compressed images are the challenges in the information security.

1.4.2 Image based steganography

Digital image steganography entails the hiding of secrete message communications between two parties. Hence, Image steganographic system embeds secret information in unrestricted cover media so it may not stimulate hacker’s suspicion. Any Image based steganographic techniques has two main features: message embedding capacity and imperceptibility [9]. However, these two features are trade off with each other. In addition, it is fairly hard to increase the message embedding capacity and concurrently preserve the imperceptibility of an image steganographic system. Furthermore, there are still many methods of steganography to be used with digital images that represent unconventional but shows potential steganography mediums. Image steganographic techniques aim a secure method to pass on a large amount of secret message, fairly to the cover image size, between sender and receiver. Additionally, it intends to keep away from the doubt of third parties to this kind of communication. Consequently, the proposed research work suggests new methods to improve the essential features of image steganographic systems. Therefore, some of the digital image characteristics have been engaged to increase the steganographic message capacity and improve the stego image quality (imperceptibility). The following sub chapters related to image steganography focus a broad introduction to the research work by first presenting the research background and motivations in image steganographic algorithms followed by the identified research problems of the research study.

1.4.3 Image Steganographic notions

The aim of image steganography is to conceal a secrete message inside a cover image in a secure manner, such that the existence of the hidden secrete message in the resultant stego image cannot be detected by attackers except the receivers [33]. All the image steganography systems follow the standard terms irrespective of the data hiding algorithms by which they are employed.

An image is a collection of discrete points which comprise different light intensities areas of the image.

Cover Image: It is the multimedia element such as text, image, audio, video and other multimedia contents and the carrier of the hidden secrete message. The choice of a cover may be selected.

Stego Image: the resultant image that carries the secrete message during the communication process.

Stego Key: The stego key refers the agreement shared by the sender and receiver during steganography process (hiding + communication + extraction) to maintain the security level of image steganography system.

Embedding Domain: It is the multimedia content where the data embedding happens in pixels or frequency coefficients or channels.

The principle of image steganography system functions under the general strategy proposed by researchers by considering Alice (Sender), Bob (Receiver), Wendy (Adversary) scenario [16].

The sender wants to transmit secrete information to the receiver by randomly selecting risk-free cover object. Then, sender hides secret information inside the cove object and perhaps uses a stego key. Accordingly, sender gets a stego object that must be identical to original cover object exclusive of suspicion. The stego file corresponds to the cover file along with the secret information. After that, sender sends a stego file to receiver over the communication channel. The goal of steganography system is to prevent adversary from perceiving the existence of communication inside the stego file. Receiver retrieves the secret information since receiver knows the data hiding technique and stego key applied in hiding process. The stego key is only shared by sender and receiver and prompted during the embedding process. An adversary can perceive secret information inside the stego file and determine the embedding pattern but they never extract the secret information if not sender or receiver has the corresponding stego key. The General principle of image steganography system is depicted in terms of the above the Alice, Bob and Wendy scenario in the Figure 1.3.

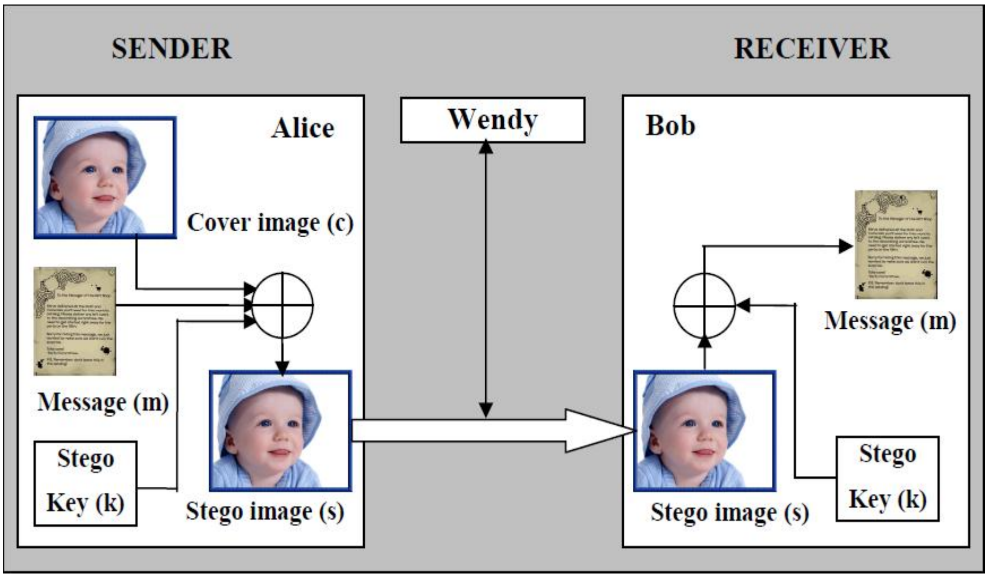


Figure 1.3: General Principal of image steganography system [34].

The security of any steganography system should suit kerckhoff's standard [35]. Hence, the assumption that an adversary has full knowledge of embedding and extraction of the process of steganography will determines the security of steganography system. However, third parties only miss the stego key to guess that the secrete communication is happening. At present, most of the steganography systems follow this principle. When the both stego keys for embedding and extraction are same, it is called symmetric steganography and when those are different, it is called asymmetric steganography.

1.4.4 Fundamental properties of image steganographic systems

The two major requirements of any image steganographic systems are, security or un-detectability and embedding capacity, which must be investigated in order to evaluate the efficiency of steganographic systems [36]. The embedding capacity is the total number of message bits to be hidden inside a cover image and the un-detectability refers the complexity of detection of secrete message inside the stego image. Therefore, the crucial aim of the image steganography is statistically undetectable with embedding large volume of secrete message.

Imperceptibility

Generally, an image steganographic method is ineffective if the third parties aware about the existence of concealed information or if the opponent suspects about the embedding technique [9].

Consequently, in the presence of secure image steganography system, visual or statistical attackers are not able to perceive the existence of concealed message inside the stego image. That means, perceptual and statistical surveillance of hidden information inside the stego image must invisible to keep away from any suspicions of attackers. On the other hand, an image steganographic method is completely secure, if the statistics of both cover and stego images are same. This will lead the quality degradation of stego image. The abnormalities of statistical features of stego image is compared to original image features by third parties to present the existence of secrete communication. Anyhow, it is difficult to get the original data hiding pattern. Therefore, the image steganographic research keeps the balance of statistics mismatching to utilize the data hiding. It is the major challenge addressed in image steganographic studies. Hence, the un-detectability refers that the embedded message is not visible to third parties that means cover and stego images are identical perceptually and statistically. The image steganographic system refers to be secure if the un-detectability of the presence of hidden information inside the stego image by perceptually and statistically. The quality of stego image compared with original cover image determines the security of the image steganographic method [37]. Eventually, it is concluded that the imperceptibility of image steganography is about the degradation of observe quality of stego image by hiding secrete message inside the cover image can be perceived by human vision system.

Embedding capacity

The upper limit of secrete message bits to be hidden in cover image without degrading the image quality and less attention of existence of message inside the stego image is called embedding capacity [38]. Hence, it is an essential requirement to employ high embedding capacity in cover image with maintaining image fidelity.

The size of the cover image determines the amount of secrete message bits inside it based on the image quality parameters. The main concern in any image steganographic system is to increase the embedding capacity without interrupting the statistical features of stego image.

Robustness

Robustness is the ability of the hidden message to keep in unbroken manner if the stego image endures some image processing activities such as filtering, scaling, addition of noises, rotation and compression [39]. Most of the image steganographic systems use internet and other computer networks as communication channels which has no degradation. Thus, the receiver obtains precisely what the sender send. Robustness is considered as desirable when the communication channel is imprecise by generating channel noise or any other interference to avert the process of steganography. Since, most of the image steganographic systems in literature follow the passive warden scenario; the design of image steganography techniques does not focus robustness as an important requirement. Image steganographic systems are limited robustness against technical modifications of image such as compression and format conversion.

Security

The goal of image steganographic communication is to conceal the simple presence of a secrete message inside the cover image without third parties suspicion. The security of image steganography beyond un-detectability and imperceptibility specifies that the hidden information could not be extracted after detecting the secrete communication in stego image. It depends on the sufficient knowledge of hiding s that algorithm and distribution of secrete keys [40].

An image steganographic system aspires to augment the trade-off between the embedding capacity and imperceptibility of hidden information in stego image [40]. The problem found in the literature between the embedding capacity and imperceptibility is seen when the large size of secrete message is hidden in cover image the quality stego image will be degraded. Furthermore, the simultaneous operation that keeps the maximum embedding capacity with good image quality is not possible due to the exchange that the artifacts generated in cover file by embedding effect. Hence, the image steganography systems must fundamentally keep the balance between the embedding capacity and imperceptibility. However, an image steganography system is not required to attain high robustness forever, but high embedding capacity with good imperceptibility must always be assured.

1.4.5 Image steganography methods

In recent times, many image steganographic techniques have propagated in information hiding domain for the solution of information security. These techniques are differentiated based on the mechanism of data embedding core of the techniques. Three main types of image steganography are identified in the research studies of image based steganography. They are spatial domain, frequency domain (transform domain) and adaptive steganography [42]. In this sub section, the key points in the frequency domain techniques are discussed to motive into our proposed research work.

1.4.5.1 Image steganography in spatial domain

For a given cover image, it is essential to find the elements in image region that might be rebuild with no considerable effect to employ data hiding. Spatial domain techniques directly modifies pixel values to embed secrete message such that the pixel values are altered to store secrete message [43]. Least Significant Bit (LSB) is the most used method in spatial domain. Spatial domain techniques also known as substitution methods consist of simple philosophy that produce a secure channel in some regions of cover image where the alterations are to be imperceptible to the human vision system.

Least Significant Bit replacement method (LSB)

LSB replacement method is a simple form of technique in which LSB of pixel value in the cover image is modified by the secrete message bits in order to embed data [44]. The benefit of this approach is easy to implement and high perceptual efficiency.

Generally, LSB does not increase the resultant file size but the resultant image size will be depend on the length of the secrete message to be concealed and also shows the noticeable changes with regarding to replacement of bits. The usage of LSB is highly influence on spatial domain techniques and also using LSB in spatial domain is vulnerable to minor changes then easily detect by steg-analyzers. LSB substitution method typically will not lead to increase in the file size, but depending on the size of the information that is to be hidden, the file can become obviously indistinct.

Pixel Value differencing method

This technique relates with adjacent pixel differences and the cover image is sub divided into separated blocks which are overlapped contained two connected pixels. The difference between the two connected pixels is used to hide the secrete message in this technique. High difference enables more possibilities of alterations [45]. Region of the pixels determines the data hiding capacity. In edge area, difference is high and it enables high embedding capacity. While, in smooth area, difference is low and it enables low embedding capacity. The imperceptibility of the resultant image is depended on the difference between the connected pixel values in each block and it keeps better imperceptibility for edge based images.

Gray level modification techniques

This technique maps the secrete message bits into the cover image pixels by pertaining some modification in the gray values of image pixel [46]. This technique will not embed the data, instead it maps the secrete data into cover image by using mathematical formula in order to keep the imperceptibility. A group of pixels in odd or even manner map into cover image by using this mathematical formula or equation. This technique achieves high embedding capacity with acceptable image quality.

Prediction based steganography technique

Pixels values of the cover image are predicted with aid of a predicator. This technique eradicates the ambiguity of other spatial domain techniques which relates directly hides secrete message into image pixel values [47]. It uses prediction error values which are altered to hide secrete message in terms of maintaining high capacity and good visual quality.

Quantization index modulation technique (QIM)

Quantization index modulation is to embed the secret information in cover image by modulating an index of pointers with the hidden information and then quantize the host image with the relevant quantizer [48]. This technique has high payload capacity and allows the message hider to manage the robustness and generated distortion while hiding the secret information.

1.4.5.2 Transform domain steganography

The transform domain techniques translate the image representation from spatial domain to frequency domain when hiding hide secrete data. In transform domain, the digital image is represented as combination of low and high frequency components. The plane and smooth regions represent lower frequency components while the sharp and edge regions concern with high frequency components. Generally, lower frequency region is more responsive since any alterations in that region will be obvious to human vision system (HVS) [49]. Therefore, embedding efficiency is varied in both lower and higher frequency regions. These concerns are the motivations to achieve the efficient steganography method in transform domain. In the literature, it has been observed that transform domain techniques are robust against attacks. To acquire the transform domain representation, the image transformation is planned to hold two important properties, reduce image redundancy and insignificant parts of image by dividing in different frequencies in image. Transform domain techniques represent that lower frequencies correspond to considerable image features and higher frequencies represents insignificant image features. The cover image which can be used as message carrier is used as an input and it is decomposed to obtain transform coefficients by forward transformation. These obtained transformed coefficients can be modified to embed secrete message. With the aid of data hiding algorithm, secrete message can be hidden in appropriate transform coefficients. To extract the hidden message in stego image, the inverse transformation is applied to recover cover image and extract the secrete message. There are lots of transform domain techniques available such as DCT, DWT, DFT, Hadamard transform, integer transform, contourlet transform etc., to employ image steganography [50]. The choice of the transformation and optimal data hiding strategy in specified frequency components are the two factors to evaluate the performance of steganography systems. In transform domain image steganographic techniques, soft computing tools such as neural network, fuzzy logic, optimization techniques etc are used to improve the essential requirements, embedding capacity and imperceptibility.

1.4.5.3 Adaptive steganography

Adaptive steganography involves a procedure that extracts the statistical features of image to interrelate with spatial or transform domain components to embed secrete message [51]. The random adaptive selection is used to identify the pixels in spatial domain or transformed coefficients in frequency domain prior to data hiding process. The goal of this adaptive steganography is to prevent the smooth area in the image to hide the secrete data. Adaptive image steganography can be grouped into three categories, texture features, HVS characteristics and evolutionary algorithms.

In case of texture features, the cover image's features are preferred when hiding the secrete data inside the cover image. Further, this approach identifies most relevant regions such as texture, high contrast and gray level variation of image based on statistical features of image to conceal the message. These regions of the image are very noisy area, accordingly, suspicion or detection of hidden message inside the image will be hard. Image steganographic techniques entail fundamental requirements such as imperceptibility, embedding capacity and these are the conflict requirements in data hiding process. The solution to this conflict is provided by the integration of HVS in the process of image steganography. HVS models integrate hidden information inside the cover image and identify perceptually important components of cover image to hide secrete data [52]. Eventually, these identified features or components are scaled prior data embedding process to keep the balance between the imperceptibility and embedding capacity. Evolutionary algorithms use optimization techniques by following a randomized process. Mainly, Genetic Algorithm is applied to choose best region or location to distribute secrete data with minimizing error in resultant image.

1.4.6 Evaluation of image steganography

The procedure of assessing the performance of image steganographic system is essential to make a solid judgment. The two important guidelines are considered in image steganographic systems to assess the performance in the literature [53].

1. The quantity of secrete information to be embedded in cover image
2. The level of difficulty of detecting the secrete message in stego image.

The evaluation of these two guidelines finds the best steganography system which can hide more data without affect the image quality.

Embedding capacity estimation

It is necessary to understand and find the quantity of secrete message measured in number of bits can be hidden in the cover image in terms of good imperceptibility [54]. It is measured in bits per pixel or bits per coefficients or bits per image blocks or regions based on the embedding method. The image steganography aims to determine the maximum amount of bits to be hidden in image components for undetectable manner. When tradeoff exists between the embedding capacity and imperceptibility, the technique used in image steganography is not considered to be worth technique if the hidden secrete message is high and the resultant image is lead to more distortion.

Evaluation of imperceptibility

The undetectability of secrete message inside the stego image refers the no visual variation between the cover and stego image and the quality of the image. The considerable visual variation in stego image lessens the unwanted suspicion of image while considering the image quality improves the level of undetectability of secrete message inside the stego image. The imperceptibility of image is depend on the perception of HVS quality. If the stego image quality is high, the developed image steganographic system's imperceptibility is high. Thus, the image quality is an important evaluation technique to assess the performance of image steganography system [55]. Objective quality assessment is one of the techniques used to aim at giving computational assessment in evaluating similarity between the cover image and stego image. The subjective quality assessment uses image quality score to assess the image by using HVS [56]. In this research, objective quality measure was utilized to evaluate the system's performance.

Object quality measures

The target of objective quality measure is to predict the perceived image quality. Based on the availability of cover image on the internet, the object quality assessment can be divided into three types. They are full-reference (FR), no-reference (NR) and reduced-reference (RR). The cover image and stego images are available in FR or NR. In contrast, stego image and supportive information about cover image are available in RR. In most of the image steganographic research studies, it has been observed that the Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) are the two metrics commonly used to assess the quality of image and compression [57] .

Further, the PSNR is used under different type of distortion environment. However, in color image steganographic systems, these two measures do not present sufficient results in terms of image quality. Since, the method works with gray images, the PSNR is used to evaluate the image quality. PSNR and MSE are the two widely used FR objective quality assessments. PSNR computes the similarities between the cover image and stego image and the PSNR calculation concerns how the cover image is close to stego image, whilst MSE computes the statistical difference in the pixel values between the cover image and stego image [58].

The mathematical description of MSE and PSNR as follows:

$$MSE = \frac{1}{M \times N} \sum_{\mathrm{i}=0}^{\mathrm{M}-1} \sum_{\mathrm{j}=0}^{\mathrm{N}-1} \left| C_{ij} - S_{ij} \right|^2 \qquad (1.1)$$

$$PSNR = 10log \frac{f^2}{MSE} \qquad (1.2)$$

Where,

C_{ij} and S_{ij} are the ith row and jth column pixel in the cover image and stego image respectively. *M* and *N* represents height and weight of both images. The value of *f* refers the maximum pixel value of image and it is depend on the depth of the image. For a gray image, the value of *f* takes 255 as maximum intensity value of gray images is 255. Image steganography systems concern to be secure if the difference between the cover image and stego image is insignificant. In such case, the quality of image is best if the value of MSE is close to zero or very small. In the PSNR evaluation, image steganography systems consider the range 20 to 40 as typical values. The image steganography system is better degree of embedded message imperceptibility if the PSNR value of stego image is high. From the literature, for gray images, the process of detecting any significant changes between the cover and stego image is difficult if the derived PSNR value beats 36dB. The proposed method competes with the PSNR value 36 dB for gray images

1.5. JPEG steganography

In the design of all image steganography systems, the primary goal of steganography that is to maintain stego file from attackers suspicion of existence of the secrete communication is the major key point to align with the characteristics of human vision system [59]. Therefore, the efficiency of image steganography system relies on the boundaries of the human vision system in order to increase the payload. From the literature, the noisy area and edge regions in images are the candidates for data hiding rather than smoother area since human vision system is most sensitive to smoother area [60]. In frequency domain, especially in DCT domain, the Human Vision System is most sensitive to noisy area of lower frequency components rather than higher frequency components as the energy of natural images is concentrated in the lower frequency area [61]. This makes that the generated distortion by data hiding in higher frequency area is visually acceptable. Thus, data hiding in lower frequencies in DCT domain is a challenge in literature in order to hide secretes data as the lower frequency area is most sensitive to human eyes. The solution to this problem is how to use HVS characteristics to identify redundancy and imperceptible area in images to be employed steganography. The proposed work relates with data embedding in lower frequency area to hide a maximum payload with good imperceptibility by investigating some image quality parameters based on the HVS and also the proposed method focuses on hiding the maximum size of the secret message by maintaining the good imperceptibility level. The research question is to derive an improved method to develop a secure JPEG steganography method that preserves the imperceptibility while increasing the embedding capacity and robust to message analyzers in terms of quantization table modification. In this work, a statistical model is presented by investigating some images features and this model finds the data hiding pattern in lower frequency area that hides maximum size of the secrete message without degrading the image quality.

1.5.1 DCT based steganography

The mathematical concept of DCT is simply referred to as a finite sequence of data points with regard to the summation of Cosine functions oscillating at dissimilar frequencies [62]. DCT presents general orthogonal transformation for signal processing and image processing. The DCT is used to convert the spatial information into frequency or spectral information. Hence, the information existing in the image can be manipulated for compression. In image steganography, the higher order suitable DCT transformed coefficients are merged to hide secrete message and it provides high compression ratio small bit error rate. Image steganography uses DCT for lossy compression environment as DCT shows strong energy compaction property that means the concentration of signal information be liable in lower frequency components of DCT domain. The DCT process generates sub-bands (lower, middle and higher frequencies) in order to maintain the visual quality of an image. The most sensitive components in an image fall in lower frequency sub-band, while the insignificant components of an image fall in higher frequency area [63]. In terms of visual quality of image, the insignificant parts are frequently eradicated by using compression techniques or noise addition techniques. In order to keep the balance between the embedding effect and visual quality of the image, DCT intends to hide the secrete message along the sub-bands in frequency domain. The data hiding in middle frequency sub-band will not unfavorably affect the quality of the image [64].

1.5.2 DCT and JPEG Compression

The evolution of digital technology has directed digital images for their huge benefits for representing, processing and viewing behaviors in different applications. The representation of digital images using digital technology is leading the generation of numerous data that means the actual image size is increased. The one of the solutions for this issue is to compress the digital image representation. The important requirement of any image compression technique is especially high degree of compression ratio without degrading the image quality. All of the image compression techniques focus on the usage of insignificant information in digital images. The identification of redundant information in digital images due to the correlation of pixels can be used to redundant information in the image. This redundancy of information in the image can be used to envisage the pixel values where the compression technique is applied. The JPEG compression technique use lossy compression procedure and is based on Discrete Cosine Transformation (DCT)

[64]. This is not only reducing the file size but also focus on image quality based on human visual system.

In the process of JPEG compression, the first step is preparation of image blocks. The actual image is represented by different color models and RGB is mostly used one that represents combination of three primary colors, red, green and blue. This model corresponds to the characteristics of human visual system as human eyes have responded to these three colors. The other color formats, especially, YC_bC_r is appropriate for image processing activities. Each pixel values range from 0 to 255 in this model represent by one intensity component (Y) and two hue chroma components (C_bC_r). The JPEG algorithm first converts RGB to YCbCr. Y is the luminance component and C_b and Cr are the red difference and blue difference chroma components. The intension of gray scale image considers Y component in the YC_bC_r. Since the human eye is less sensitive to chrominance than luminance, the algorithm takes advantage of this red sub-samples values C_b and Cr without significant visual degradation and can average four chrominance pixels resulting in better compression of C_b and C_r. The RGB to YC_bC_r conversion is lossy but imperceptible to human eyes. With the intention of faster and efficient transformation, the original image after RGB to YC_bC_r is arranged by square blocks of size 8x8 pixels. Each block has 64 image pixels that mean 64 different light intensity values [65]. The 8x8 block preparation is preferred based on the satisfactory results ever since during the establishment of JPEG standard, the increment of blocks size were not possible because of the too much hardware requirements and computation time. The shrink of block size from 8x8 to 2x2 or 4x4 is not suitable because of the DCT interfered less effective in compression algorithm. After partition the image into 8x8 non overlapping blocks, the two dimensional Discrete Cosine Transformation (DCT) is applied to each blocks. Each blocks received signal intensity in 64 levels and these intensity levels are produced as 64 coefficients in each blocks. An alteration of a single DCT coefficient in each block will affect the image pixels in relevant block [66].

The first coefficient in each block represents the average intensity value of 64 coefficients termed as DC coefficients, while the rest of the 63 coefficients are called AC coefficients. The more details of the image data fall in DC coefficient and also

DC coefficients in each block are very important to reconstruct the image during the JPEG compression process. AC coefficients near to DC coefficients in each block are termed to lower frequency coefficients which are most sensitive to human vision system. The AC coefficients in bottom right part are called higher frequency coefficients that are less sensitive to human vision system. DCT does not affect loss of image data. Inverse DCT should restore the original contents with negligence of error value as the DCT is fully reversible. Eventually, after applying DCT into each block, the lower frequency coefficients gets the higher value since the image data concentrated in lower frequency area and higher frequency coefficients obtains lower values [67].

The next step of JPEG compression process is the quantization stage. All the DCT coefficients in each block are scaled by dividing the integer values which represents as a quantization table. It is called quantization process. The range of these values is 1 to 255. After that, the divided coefficients termed as quantized coefficients in each block are rounded to nearby integers. The quantization step is a lossy part of the JPEG compression due to the rounding error [69]. The standard JPEG quantization table used in JPEG compression is listed in the Chapter 3.

The JPEG standard quantization table is a two dimensional matrix which have 64 integer values and we can alter these 64 values to keep the requirements of compression technique. It is the default quantization table for luminance components of image. The values in the quantization table are increased diagonally because of more details of image are removed. The actual purpose of quantization is to quantize the values that represent the image in transform domain. The 64 DCT coefficients in each block are divided by quantization table individually and the results also rounded to nearest integers to eliminate the redundant transformed coefficients [69].

After the quantization process, in each block, few coefficients get values in lower frequency area, remaining coefficients get number of zeros. To align same frequencies in order to provide efficient compression, the quantized DCT coefficients are arranged in Zigzag manner. By applying the zigzag order to quantized DCT coefficients, the insignificant coefficients are rounded to zero while significant coefficients lose their accuracy. The entropy encoding process in JPEG which contains Run-length encoding, Huffman coding to compress AC coefficients and

DCPM to compress DC coefficients in each block is applied after arranging quantized DCT coefficients in zigzag manner. Finally, the JPEG compression scheme achieves compressed data [69]. The quantization process is lossy compression technique while entropy encoding process is a lossless compression technique. This will motive for JPEG steganography that selects the suitable stage in which embedding process is happened. The compressed JPEG file contains a quantization table, Huffman table and other compressed data inside the header part of the file.

To reconstruct the original image, the JPEG decoding process is initiated. The JPEG file is entropy decoded using the Huffman table and other supportive data available in the JPEG header file. The entropy decoding process does the process of decoding of DCPM, decoding of Huffman coding and decoding of run-length coding. After this process, quantized DCT coefficients in each block are recovered. By applying de-quantization process, the DCT coefficients in each block are obtained. To reconstruct the image in pixel domain, inverse discrete cosine transformation is applied to each block [70]. The JPEG encoding and decoding process is illustrated in the Figure 1.4.

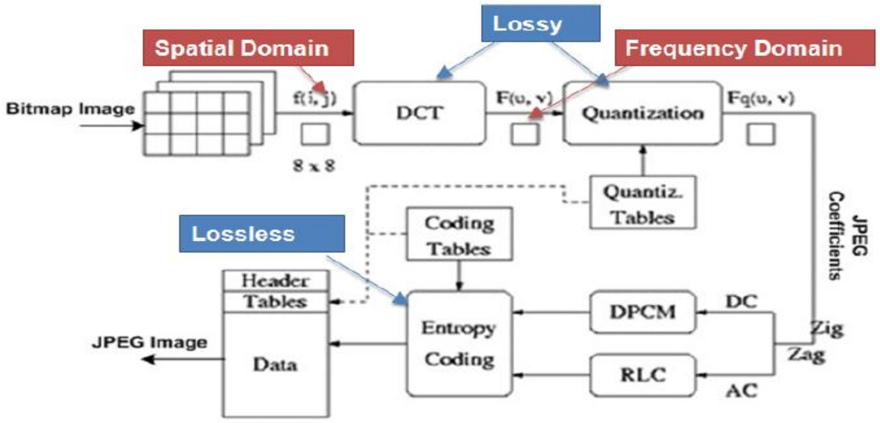


Figure 1.4: Block diagram of JPEG compression showing the lossy and lossless stages during the encoding process [69].

1.5.3 Steganography in JPEG domain

The two main categories of image steganography are the spatial domain and transform domain techniques. LSB coding is the primary technique used in spatial domain image steganography. JPEG transforms spatial data to transform domain to achieve the compressed JPEG file by lossy and lossless techniques. Data embedding in spatial domain by using LSB causes to bring in too much distortion and to introduce errors during the extraction of hidden data in spatial domain [71]. By these reasons, steganography would not be achievable with JPEG images due to its lossy property. However, the motivation for JPEG steganography is the JPEG encoding process in frequency domain in which the lossy and lossless compression stages are taking place [72].

The spatial data to frequency domain by DCT and quantization stages are lossy, while entropy encoding which includes RLE, Huffman Coding and DPCM of quantized DCT coefficients are lossless compression [69]. The space between the lossy and lossless compression is utilized by researchers to hide secrete data bits inside the JPEG coefficients in JPEG steganography [73]. The data hiding takes place in quantized DCT coefficients between the quantization process and entropy encoding process. The illustration of JPEG steganography and its data hiding phase is outlined in Figure 1.5.

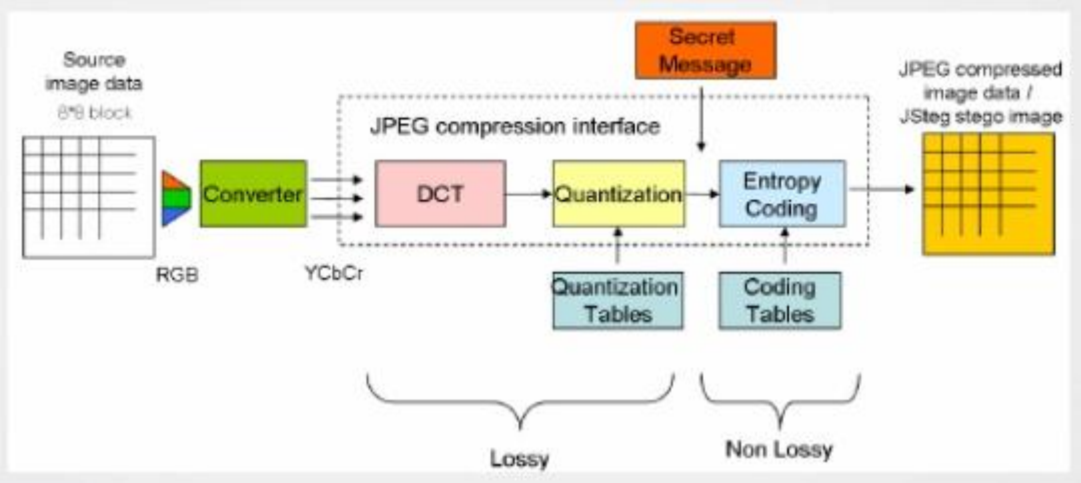


Figure 1.5: The JPEG Steganography process **[72]**.

An embedding method that hides secrete data in JPEG image is to modify the DCT coefficients to imitate the secrete data bits. After hiding secrete data bits inside the quantized DCT coefficients, the resultant coefficients with secrete data bits are encoded by entropy coding to create JPEG stego image. By hiding secrete data in JPEG coefficients which fall in lower frequencies or middle frequencies or higher frequencies listed in Figure in compressed bit stream, it is tricky to detect the existence of hidden data as the alterations are generally not observable by the human vision system in pixel domain or spatial domain and secrete data bits will not be destroyed. Thus, the embedding techniques in JPEG images are more robust and secure. The trade-off between the imperceptibility, embedding capacity and the compression ratio is managed to scale the DCT coefficients by adjusting the quantization table values in quantization process. Conversely, the extraction of secrete data in JPEG coefficients is the reverse process of entropy encoding called entropy decoding process. The JPEG stego file is decoded by entropy decoding process that includes decoding DPCM, decoding Huffman coding and decoding run-length encoding to recover the quantized DCT coefficients to extract the secrete data bits as the decoder has a secrete key to identify the coefficients in which data hiding happens [74].

Another way to extract the secrete data bits inside the JPEG is to restore the JPEG stego image to spatial domain and then apply the few stages to restored image to extract the secrete data. First, the JPEG stego image is entropy decoded to attain quantized DCT coefficients. These coefficients are multiplied by quantization table to restore the DCT coefficients. It is called de-quantization. Then apply inverse cosine transformation to get spatial image. This spatial domain image is again divided into non-overlapping blocks and then applies DCT to each block. The quantization step is again applied by same quantization table. At this stage, decoder extracts the secrete data based on knowledge shared by sender. This extraction process extracts the message without destroying and restores the resultant image by using the similar quantization table used in this process [73] .

The JPEG steganography faces some challenges in order to satisfy the requirements of image steganography system such as imperceptibility and embedding capacity while keeping the good compression ratio. The selection of appropriate coefficients in frequency area is one challenge to embed secrete message with satisfying image steganography requirements [74]. Another important challenge in JPEG steganography is the modification of quantization table in order to keep the high embedding capacity and good imperceptibility with reasonable compression ratio [75]. The quantization table modification is done in two ways in favor of JPEG steganography. First, the raw image is compressed with modified quantization table and secrete message is hidden during the compression process. Another way of hiding is entailed in JPEG compressed images. This will cause double compression effect. The primary quantization table used in JPEG images is modified in this process to enable the data hiding. The second one is highly competitive to keep the balance between embedding capacity and imperceptibility [76]. The proposed approach works with compressed images to investigate the impact of data hiding in lower and middle frequency DCT coefficients by modifying existing quantization table called primary quantization table in order to achieve the high imperceptibility while enhancing the embedding capacity. The compression ratio is optional in our approach as higher frequency coefficients are ignored for data hiding.

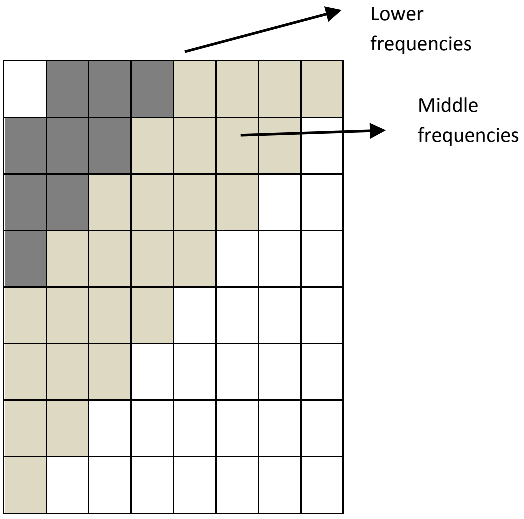


Figure 1.6: Frequency locations in a DCT block where embedding takes place in proposed method.

An adversary or attackers may guess in some resultant images and may perceive the presence of hidden communication inside that image. To prevent this, the image steganographic systems focus the characteristics of human vision system (HVS). The HVS is most reacted to lower frequency coefficients and the energy of image is concentrated in lower frequency coefficients [75]. Thus, the data embedding in lower frequency coefficients is a difficult process to balance the trade-off between the imperceptibility and embedding capacity. The higher frequency coefficients are discarded after quantization step. Therefore, the steganography process will choose the middle frequencies as appropriate places for data hiding to achieve the efficiency.

LSB data hiding method is the widely used common technique to hide secretes message bits in pixel value or DCT coefficients. The least significant value of image content is modified to zero or one with relevant MSB of secrete message bits. By this embedding process, the actual pixel or coefficient value will be increased or decreased. The receiver then retrieves the secrete message bits by reading the coefficients in proper order and decodes them based on the secrete key shared by sender. The advantage of LSB data hiding in frequency domain is the high embedding capacity and the alterations by hiding are visually undetectable by HVS. The LSB technique enables one bit per coefficients in each block. This can provide a higher capacity rather than spatial domain and reduce the suspicion on stego file by attackers if the stego image is small. Therefore, most of the image steganography techniques practice the data hiding bits directly in spatial domain. Therefore, LSB is preferred in JPEG steganography.

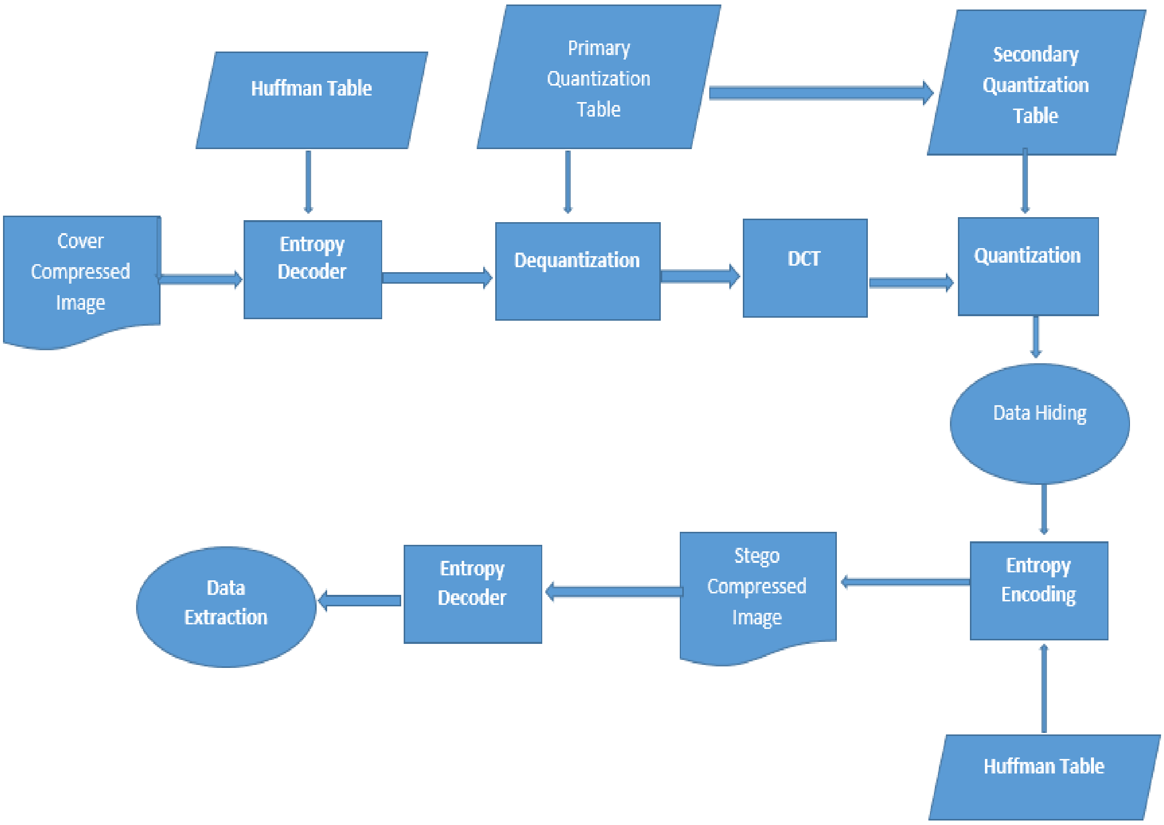


Figure 1.7: Block diagram of the process JPEG steganography in compressed domain

1.5.4 Influence of quantization process in JPEG steganography

JPEG compression technique works with pair of 8x8 quantization tables (luminance and chrominance) which are not default tables. The determination of values in quantization table is a challenge in JPEG steganography in order to achieve the correlation between the requirements of steganography based on the effect of data hiding [77] . The quality of image and compression ratio is derived by applying quality scaling factor to quantization table. The human vision system is more responsive to lower frequency area as the energy intension in natural images falls in lower frequency components. The careful consideration of quantization step in upper left part of quantization table preserves the DCT coefficients to achieve invisibility of secrete message inside the cover image even as it populates higher frequency DCT coefficients to zeros to eliminate the information that is visually insignificant [75].

The human visual system (HVS) is more responsive to lower frequency noise since the energy of natural images is concentrated on the lower frequency components. In image compression with a JPEG baseline system, the quantization step preserve the DCT coefficients needed to achieve the desired image quality whilst it zeroes out most of high frequency DCT coefficients and discards information that is visually irrelevant. Consequently, the selection or modification of quantization table in JPEG steganography is highly motivated in research studies to determine the quality of image, embedding capacity and compression ratio during the data hiding process. Most of the researchers use arbitrarily generated quantization tables in their research studies. Several methods have been developed to find the optimum quantization table in JPEG compression technique. But, in JPEG steganography, embedding capacity is an extra requirement with image quality and compression ratio to find optimum quantization table. Therefore, find the optimum quantization table in JPEG steganography is a challenge and it does not fall in other methods used in JPEG compression technique.

The well-known JPEG steganographic technique is Jpeg-Jsteg that embeds the secrete message in the LSB of quantized coefficients whose values are not equal to 1, -1 and 0 in each block [78]. It suffers from the problem of embedding capacity. Since the energy of cover image is on lower frequency coefficients, modifying those coefficients to improve the embedding capacity will lead the quality degradation of stego image. The higher frequency coefficients always are zero due to quantization process. To solve this problem, the quantization table is modified by researchers to improve the embedding capacity with reasonable image quality. Chang et al. proposed a quantization table modification technique with the intention of improving embedding capacity compared with Jpeg-Jsteg [79] . Further, this technique modifies two LSB bits of middle frequency coefficients with secrete message bits in each block while Jpeg-Jsteg modifies one LSB bit of quantized coefficient with secrete message bits. This technique is the root method for quantization table design and modification techniques and it achieves improved embedding capacity and group of coefficients selection for data hiding.

1.5.5 Optimization of quantization tables in JPEG steganography

In JPEG steganography, it is observed that the quantization table determines the image quality, embedding capacity and compression ratio during the data hiding process. Hence, it is essential to find an optimized quantization table with better quality of image than existing quantization table in JPEG process with embedding effect. There are some methods found in literature to find optimized quantization table rather than default table. The investigation was done to find a relationship between quantization tables and restored JPEG image quality in [80]. The quality of JPEG image was assessed by modifying the quantization table value in each band of quantization table which is partitioned into four bands based on the frequency. Finally, it was found that the DC coefficients in each block have considered affecting the image quality. Another optimization technique was proposed by Yuebing et.al [80] that uses the statistical method to propose quantization table in order to improve the compression ratio.

Chang et.al designed an image independent quantization table to achieve perceptual quality of resultant images based on human vision system by evaluating the PSNR. A model presented to generate quantization table to improve the PSNR of the reconstructed image.

Eventually, it is concluded that the optimized quantization tables significantly improve the compression ratio and image quality than using default table. By applying these optimized quantization tables to JPEG based steganography, the stego image gets better quality by embedding more bits. These techniques are the general techniques and these techniques are also categorized based on the approach of generating quantization table. In most of the quantization table modification techniques except random modification techniques, some elements of the quantization table values are scaled in order to compare the DCT coefficient value to find the embedding efficiency.

Specially, in double compression JPEG steganography environment, data hiding in lower frequency coefficients is tricky process which causes quality degradation [83]. This allows that some coefficients are used to hide the data by modifying existing quantization table in compressed image to maintain the image quality with acceptable embedding capacity.

Our proposed method will give more possibilities to gray images in case of quantization table modification. The top left are of quantization table values are divided by three factors to produce a range by using default table used in image set. Every modified table is experimentally investigated with randomly generated data hiding patterns in lower frequency area.

The quantization table modifications techniques are categorized into two ways in the research of JPEG steganography in terms of the compression process. The first one is single compression JPEG steganography and another one is double compression JPEG steganography.

The single compression JPEG steganography technique only embeds modified quantization table inside the JPEG header file and receiver extracts the hidden message by using this table and appropriate secrete key. Apart from the image quality, third parties will observe this stego JPEG file and they suspects the quantization table modification if they have original file by comparing the original file with modified file. Otherwise, they are not able to suspect that the secrete communication is happened and cannot detect the secrete message as secrete message is hidden in DCT coefficients.

The double compression JPEG steganography differs from single compression technique in terms of quantization table modification. This process compresses the image twice with different quantization tables. The compressed image is used as cover image in this technique. The data hiding happens in two ways in this technique. The JPEG compressed image is entropy decoded and scale the recovered quantized DCT coefficients to hide secrete message. Then, the entropy encoding process is applied again to compress the image [76]. This type of hiding is not related to quantization table modification.

Another technique is to use secondary quantization table to recompress the compressed image. The actual JPEG file is entropy decoded and the spatial image is received by applying reverse process of quantization by using existing quantization table called primary quantization table and inverse discrete cosine transformation. The de-quantization and IDCT preserve the image contents. The spatial domain image is again employed into JPEG compression by using secondary quantization table to embed data. The only secondary quantization table is stored in JPEG file and primary quantization is lost. The double compression JPEG steganography causes significant changes in resultant image rather than single compression technique as the quantization process occupies twice in the process [84]. In case of security scheme of double compression JPEG scheme, imperceptibility is an important requirement that is achieved by careful selection of secondary quantization table to hide more bits. It is high robustness against attacks then secrete message cannot be destroyed. Third parties have a challenge to find the primary quantization table in this process to suspect the secrete communication beyond the quality of the image. Attacker only observes these types of stego images and then ignore as the wider use of images in internet and good imperceptibility. Steg-analyzers may identify the traces of manipulation if they have sufficient knowledge of original image or the produced stego image causes some traces. The double compression JPEG steganography mainly focuses the imperceptibility requirement by evaluating the image quality parameter such as PSNR, MSE …etc to minimize the traces occurred in resultant image.

Finally, using JPEG compressed images as carrier file causes some challenges such as decompression, optionally transform to spatial domain, recompression which rise a number of problem to hide secrete message.

In the proposed method, it presents a practical method with respect to quantization table modification in double compression JPEG image for kind of gray images by investigating a number of secondary quantization tables with primary quantization table to improve the imperceptibility and the embedding capacity.

1.6 Model based steganography

The spatial and frequency domain image steganographic techniques have shown their potential strengths and weakness in terms of the mechanism of data hiding. In literature, it is obviously reveals the strengths of frequency domain techniques compared to spatial domain techniques. The fundamental security principle of image steganography is depending on the statistical features of stego image that imitate the existence of hidden information inside it by embedding effect and generated artifacts in the stego image that causes the attention of the attackers. To overcome this problem, another type of steganography called model based steganography is developed based on the spatial and frequency domain techniques [85] [86] [87].

The model based steganography uses spatial or frequency domain for data embedding and generates a model before data hiding. The modifications of pixel values or frequency coefficients are investigated by analyzing the statistical characteristics or other features of cover image to find the embedding locations in cover image then the model is generated based on the analysis of statistical characteristics of the cover image. Model based steganography embeds secrete message in the cover image in accordance with a model representing cover image statistics and is more robust compared to LSB replacement with regard to compression and image processing operations. The intension of model based steganography is in considering some statistical features of the cover image so as to embed secrete message with no modification of the considered cover image features. The model based image steganographic techniques should provide good embedding capacity with good embedding efficiency with preserving image quality or without detecting the secrete communication inside the stego image and also provides extra layer of security as this is less prone to attacker's attention. However, these techniques are not working full secure manner since the steganalysis process fits a model by comparing the statistical features of cover and stego image to detect the secrete communication using statistical features to detect the secrete communication [86] . Hence, the secrete message to be hidden in model based steganography should be encrypted before hiding. By this process, secrete message cannot be extracted by third parties. Finally, the adaptive steganography opens a new path to secure steganography which is analysis the important characteristics of cover image in terms of its statistical features tracked by a mathematical model and embeds secrete message according to generated model with minimizing distortion in stego image.

1.7 Solution provided by the proposed approach

JPEG steganography raises the questions with the intention of image steganography requirements in the literature. The possibility of avoiding detection of secrete communication inside the stego image by third parties is questioned on insignificant statistical features of the DCT coefficients without giving up half size of embedding capacity. The second question is asking the maximum secrete message size that can be hidden in a given cover image without detecting the secrete communication in stego image. Third question is related to the procedure that can achieve maximum embedding capacity. To answer these questions raised in literature, the solution is provided by modeling of cover image features lead to model based image steganography. The process of JPEG steganography compress the cover image by using quantization process and after this process, the secrete data is hidden before applying entropy encoding process as entropy encoding is lossless. In our approach, the double compressed image is provisionally converted to spatial domain and applies modified quantization tables to compress the image again with enabling the data hiding. This proposed technique works with lower frequency area data hiding for gray images. By combing experiments, for an image, we find the modified quantization table with relevant hiding pattern by combining four quantization tables with fifteen data hiding patterns. The joint statistical features that include DCT features of lower frequency area and some statistical features of spatial domain are extracted and experimentally investigated with the quantization table and data hiding pattern by using statistical analysis software to identify the correlation between them. Some positive correlation values found among the several combination of testing. Those correlated features are used to fit a model. In passive warden scenario, message analyzers are enable to observe the stego object and are not allowed to modify the stego object. The proposed model based steganography uses the model to embed data and the same model is used to extract the data at the receiver side and it does not send key to the receiver over the secrete channel. Hence, the proposed method is a passive warden scenario. According to correlated features of cover image, this proposed model is used to select the maximum message size to hide in cover image without degrading the image quality. The detailed description of proposed model based steganography for JPEG images will be discussed in chapter3.

1.8. Motivation and research problem

Digital image steganography using JPEG format faces the significant challenge with regarding to size of cover image which limits the embedding capacity. Additionally, the concealment of secrete message in JPEG cover image may alter the characteristics of cover image. These alterations are visible to HVS and attract the attacker's attention. However, amount of hidden data in cover image is increased; the stego image is more suspicious by attackers. Thus, the design of JPEG steganographic techniques should consider the tradeoff between the imperceptibility and embedding capacity. In the JPEG steganography process, the quantization table design or modification plays the vital role in order to evaluate the performance of system. The quantization process is done by quantization table modification. The entries in quantization table controls the imperceptibility of secrete message in resultant image and embedding efficiency without affecting the compression ratio. In the literature, Designing quantization table for JPEG compression are developed by some soft computing tools based on HVS. Modifying quantization tables in terms of data hiding is left up for researchers to employ efficient steganography. In case of quantization table modification techniques, the modification of quantization table entries are randomly modified in most of the research studies and some particular entries of quantization table are investigated with DCT coefficient and other image feature to design efficient steganography. Both of these techniques are still suffered in the selection of DCT coefficients with relevant quantization table entries. Middle frequency entries are the good candidates for data hiding by changing the middle part of quantization table entries to one. Some of the researchers have done some experiments to hide data in lower frequency area with competitive results in raw and compressed domain. According to the quantization table modification techniques made in the literature that the modification of quantization table entries in upper left part will cause the considerable significant changes while applying data hiding in lower frequency area. To solve this existing issue, this study proposes a practical method to investigate the lower frequency data hiding with relevant quantization table modifications in upper left part to give more opportunities to feasible data hiding by evaluating the image quality parameters. The proposed study method selects reliable data hiding pattern with relevant modified quantization table for set of images. The image data set falls in the same characteristics and follow same quantization table. Finally, this study investigates the image features against these selected data hiding pattern and modified quantization table in order to design a model that finds the best hiding pattern that hides more data without degrading the image quality.

1.9 Aim of the study and Objectives

The aim of this study is to investigate the quantization table modification effect with regarding to data hiding in DCT coefficients and devise a model based steganography approach in terms of quantization table modification to increase the embedding capacity without degrading the image quality.

In order to achieve the main aim, the following sub objectives are to be achieved:

- Compare the steganography with other information hiding techniques in terms of the mechanism of secure communication to facilitate the information security.
- Justify the reason to select the image steganography techniques and to provide an overview of image steganography with the essential characteristics.
- Research the JPEG steganography with the impact of quantization tables and discuss the pros and cons of the quantization process by evaluating the image steganography requirements and identify the anomalies in this related research.
- Investigate the quantization table modification in JPEG steganography and how it affects the image quality, embedding capacity and compression ratio.

- Develop a practical module to find the modified quantization table and relevant data hiding pattern for an image in order to achieve the requirements of the imperceptibility and embedding capacity.
- Model the relationship between the quantization table, hiding pattern and image features in terms of quantization table modification without perceiving the hidden communication in resultant image.

1.10. Thesis outline

The ingredients of this thesis are structured as chapters and the description of every chapter is as follows. Chapter 1 briefly introduces the information security in communication channel and it explains the need of cryptography and steganography in information. The usage of cryptography and steganography in data security problem is also discussed in this chapter. The key points of this chapter are the spirit of image steganography, properties of image steganographic system, and image steganographic techniques in different domains because of addressing our research problem in the field of image steganography. Finally, it has been addressed the identified problem statement in literature, objectives of this proposed work and scope of this proposed research study in this chapter. In chapter 2, the state of the art of current image steganographic techniques related to our proposed work are technically and comparatively reviewed on order to address the proposed method.

Chapter 3 presents the design and implementation of intended image steganographic method and it's all the features used in developing the proposed methodology.

Chapter 4 brings forward the extracted results from proposed work and their detailed discussion to defend the proposed method compared with state of the art. It presents fruitful justification of proposed method as it selected as a good method in terms of specific requirements of image steganography.

Finally, Chapter 5 presents the objectives of proposed method one more in chapter 1 and concludes the summary of proposed work with acceptable suggestions and also addresses the future directions to improve the existing method.

1.11 Chapter summary

This chapter introduces the main concepts concerning with digital image steganography and identifies the security issues, performance metrics and data hiding techniques for image steganography to strongly possess our proposed approach. Further, this chapter clearly illustrates the information hiding techniques in JPEG steganography and discusses its pros and cons. Further, the chapter 1 briefly introduces the proposed approach with comparing the merits and demerits other methods related to existing research studies in terms of requirements of image steganography. Finally, the outline of the thesis according to its ingredients is introduced to easy navigation of relevant information of the thesis.

CHAPTER 2
LITERATURE REVIEW

The steganographic techniques employed in JPEG images have been extensively studied in this chapter. These techniques are divided into two categories, the first one is data hiding in raw images and second one is data hiding in JPEG compressed images. Throughout this chapter, it has been studied and reviewed the most topical and considerable methods related to JPEG steganography and discussed the significance of quantization table modification with respect to the essential requirements of data hiding in JPEG images.

2.1 Review of JPEG steganography

Here, the raw image in any format are converted to DCT domain by dividing image into equal sized blocks then the DCT coefficients are used for hiding secrete message bits. Finally, the JPEG stego image is produced by applying JPEG compression procedure as in Chapter 1.

The comparison of LSB based data hiding in pixel domain and DCT domain were discussed in [88] [89]. The LSB based image steganography in pixel domain conceal message bits into LSB of pixels in cover image while the DCT based steganography embeds the message bits into LSB of the DCT coefficients. For all type of images, the derived PSNR is high in DCT based technique as compared with LSB based technique. It means that the DCT based scheme shows the minimal distortion compete with the LSB based technique. The embedding capacity of LSB based technique is high as compared with DCT based technique. From the experimental proof, researchers recommended that the DCT based techniques are applicable for image quality based techniques. It is obliviously identified that the DCT based technique is to aim high embedding capacity while keeping the minimal distortion. So many techniques in DCT domain were proposed in the literature to keep the balance between embedding capacity and image quality by different techniques. In case of extraction of the hidden message, LSB based technique can easily be extracted by adversary as compared to DCT based technique. To achieve the balance between the embedding capacity, image quality and less suspicious level of secrete message existence, the DCT based technique was proposed by Chu R, You X, Kong X, et al. in [90] by altering the magnitude of specified DCT coefficients of cover image and also it showed the good invisibility, high embedding capacity and less suspicious level compared with LSB based pixel domain technique. Finally, the proposed method is working with DCT based techniques which are the candidates for steganography if the alterations are done in the DCT coefficients including DC and AC coefficients. According to the philosophy, the proposed method is working based on the alteration of DCT coefficients by modifying the quantization tables in JPEG images in Chapter3.

The quantization table based secrete communication was proposed by Po-Yueh Chen and Wei-Chih Chen in [75]. The key concept of quantization in JPEG steganography is to encode the DCT coefficients by using quantization table based on the image quality factor. The size of secrete message to be embedded in transform domain is determined by adopting different quantization tables. This method illustrates the frequency domain data hiding method based on the variation of quantization tables used in quantization process. The secrete message is hidden inside the gray image based on two different quantization tables that improve to extract the hidden secrete image same as original. To improve the quality of JPEG stego image, the method incorporates DCT with DWT. The results derived from experiments showed satisfactory embedding capacity with good image quality and improved accurate extraction rate. The comparison of this method and the proposed method is the modification of quantization tables.

The dynamic approach of frequency domain based data hiding in grayscale image was proposed by Samadrita Guha & Dipti Kapoor Sarmah to increase the embedding capacity of the cover image divided into pixel per blocks transformed by DCT [91]. After quantizing the DCT blocks by standard JPEG quantization matrix, the amount of secrete message bits to be hidden in each block is derived by the block capacity identifier method. Further, researchers improved the embedding capacity of stego image by using a modified JPEG quantization matrix. The modification of quantization table increases the resultant image size than actual image size. So, the increase of file size after hiding in DCT domain by applying quantization table is a challenge for researchers to carefully determine the modification of quantization matrix. The proposed approach overlaps with this method in case of modification of quantization matrix and it solves the problem of the increased file size after hiding to certain level for gray images in compressed domain by adding more possibilities of the quantization modification techniques.

Shamim.et.al proposed a JPEG steganography method by joining substitution encryption technique and DCT based data hiding [92] . They proposed novel encryption method with substitution technique and the encrypted message is embedded in quantized DCT coefficients to produce JPEG stego image. The performance of this method was evaluated by computing PSNR and MSE. The experimental results showed the good perceptual and statistical value of the image to enable secrete communication. By adding any encryption technique on cipher text and randomization of data hiding in image blocks, our proposed method will get the additional layer of security it enables that no one detected the secrete message if they suspect some modification done.

The research work proposed by Jessica Fridrich considers the issues of active steganography and also it keeps the statistical and perceptual transparency against the attacks. The main theme of this research work is to advertise the stego image in uncompressed format while they can endure JPEG compression scheme by certain image quality factors. The secrete message is embedded in DCT coefficients by using statistical restoration framework [93]. In our method, we have advertised the stego image in compressed format. So the perceptual transparency is the first factor to secure the stego image from the visual attacks. It is the primary requirement of secure steganography system achieved by calculating PSNR values.

2.2 Quantization table based JPEG steganographic techniques

Quantization and de-quantization process plays major role in JPEG compression process in order to initiate steganographic techniques in JPEG images because of the lossy compression [94]. Quantization process keeps the DCT coefficients required to attain the preferred image quality even as it causes most of the higher frequency coefficients to zero and eliminates the irrelevant visual information in image. The values in quantization table control the image quality and compression ratio. In lossy part of JPEG compression process, before entropy encoding, quantization step determines the amount of compression and image quality [95]. This philosophy motives for optimized quantization table design for JPEG steganography. The optimized quantization table used in JPEG steganographic process may result in a reconstructed stego image with satisfying steganography requirements than using the default quantization. The JPEG compression process uses 8×8 quantization table which does not indicate default values for the compression process. Therefore, selection of quantization table values in quantization table is dependent on the application of JPEG steganography. The default quantization table for luminance (Table 1) and chrominance (Table 2) used in JPEG compression process were empirically investigated and established to show good results [96]. In the process of JPEG steganography, the quantization tables can be randomly generated and the generation of quantization table values should be imperceptible for human visual system between the cover image and stego image [97]. Finally, in the JPEG steganography, optimization of quantization tables, especially in luminance area, is vital to attain the good results such as imperceptibility and embedding capacity in terms of security of the steganography system.

Image quality is an important in the process of optimization of quantization table to maintain the balance between cover image and reconstructed stego image. A quality factor can be applied to quantization table by using mathematical equation to keep the image quality. So, the constant value can be used to divide the quantization table in most of the research studies [69]. There are several methods proposed in literature to optimize quantization table used the JPEG steganography process. Still, they are competing with the image quality since the energy of DCT coefficients in different bands (lower frequency, middle frequency and higher frequency). Imperceptibility refers image quality , embedding capacity (payload), and compression ratio are the important factors to be considered in the JPEG steganography and they have trade-off in quantization table modification process to get optimum quantization table. However, the consideration of these factors may depend on the requirement of the embedding method. The embedding method in lower frequency area focuses the imperceptibility and embedding capacity while higher frequency area hiding highlights imperceptibility, embedding capacity and compression ratio since most of the higher frequency DCT coefficients are zero after quantization process that affects the file size. The ultimate goal of JPEG steganography is secure communication. Typically, the embedding capacity of a steganography method refers the size of the secrete message transferred between the sender and receiver. Hence, most of the researchers try to increase the steganography capacity to embed much more secrete data bits in cover image in order to maintain the balance between imperceptibility and embedding capacity [98].

The JPEG compression divides the image into non-overlapping blocks of 8 × 8 pixels and transforms each blocks from spatial domain to frequency domain by applying a 2D DCT. After that, DCT coefficients in each block are quantized and entropy coded to provide compressed image [99]. In the literature, most of the JPEG steganographic techniques adopt the standard JPEG compression. There are two quantization tables used in JPEG compression process for luminance and chrominance displayed in chapter 1. The values in 8×8 quantization tables are not default and based on the application. The selection of quantization table values plays the major role in JPEG steganography in terms of image quality and compression ratio. The suggested quantization tables for luminance and chrominance are the called standard tables by keeping the balance between image quality and compression ratio.

The quality factor is applied to standard quantization table to generate different quality images in JPEG compression process by maintaining the compression ratio. In case of JPEG steganography, the hiding data in DCT coefficients is another concern competes with quality factor and compression ratio.

The HVS is the key factor that determines the image quality by applying quality factor. In DCT domain, HVS is most reacted with lower frequency area as the energy of image is concentrated in lower frequency components [100]. The quantization process brings most zeros in higher frequency area that causes discarding visually irrelevant information in image. It is oblivious that the determination of values in quantization table controls the image quality during the data hiding process. In JPEG steganographic studies, researchers are permitted to generate or modify the quantization table to control the image quality, compression ratio and embedding efficiency. Hence, the scope of quantization table modification in JPEG steganography is preferred in our research study. In JPEG steganography, the loss of image fidelity occurs during the quantization process, it is essential to optimize values in quantization table. Many research studies proposed related to quantization modification in literature. The available methods are reviewed and compared with our proposed practical method in order to address the research problem.

The first JPEG steganography method is Jsteg which is a general method for JPEG images [78]. Jsteg splits the cover image into non-overlapping blocks of 8×8 pixels and transforms each block by DCT. All the DCT coefficients in each block are scaled with default JPEG quantization table (table). It embeds secrete message bits in the least significant bits of the quantized DCT coefficients that are not equal to -1, 0 and 1 in each block of cover image in zigzag order. Receiver extracts the secrete message bits by scanning the quantized DCT coefficients whose values are not equal to -1, 0 and 1 in each block of the stego image. This method suffers from limited embedding capacity since the quantized DCT coefficients in higher frequency area are mostly zero and quality degradation of stego image due to the energy concentration of image fall in lower frequency area [101]. Therefore, the suspicion of the existence of the secrete message inside the resultant image is easily detected by chi-square attack [94].

Another JPEG steganographic scheme called outguess was developed to preserve histogram of DCT coefficients to oppose the chi-square attack and carefully selects the quantized DCT coefficients for data hiding by LSB replacement method to minimize the statistical distortion that may draw less attention of adversary to secrete message existence in the stego image [102]. Outguess spreads the embedding locations by using a pseudo random number generator to mix up the arrangement of DCT coefficients and uses half number of all quantized DCT coefficients in each block whose values are not equal to 0 or 1. With compare to Jsteg, outguess survives simple statistical attacks since it preserves first order statistics and embedding capacity is reduced as the selection of quantized DCT coefficients for hiding is reduced.

Westfeld et.al proposed another JPEG steganographic method called F5 that increase the embedding capacity without degrading the image quality rather than Jsteg and Outguess [103]. F5 does not use the quantized DCT coefficients whose values are equal to zero for data embedding and reduces the value of quantized DCT coefficient with one to hide a secrete message bit as an alternative of tossing the least significant bit of the particular coefficient. The mismatching of secrete message bit and LSB of quantized coefficient will reduce the absolute value of the coefficient to enable data hiding. Otherwise, quantized coefficient value will be preserved with secrete message bit. Additionally, F5 uses matrix encoding technique to spread the secrete message bits among the coefficients bits. The maximum capacity of F5 should not be more than 14% of the size of cover image with defending against the visual attack [104].

Sallee.P proposed a model that finds the relationship for the maximum embedding capacity and statistical undetectable of the existence of secrete message inside the stego image [105] . The non-zero AC coefficients are modeled in this method by using parametric density function. This resists statistical attacks and achieves larger capacity than F5 [103] and Outguess [78].

The solution for the Jsteg approach is the modification of quantization table to improve the embedding capacity and minimize quality degradation. Consequently, Chang et al. proposed a modified quantization table (Table 3) based JPEG steganography method called JMQT (Figure 1) to improve the efficiency of the Jsteg method in terms of embedding capacity [79]. The actual luminance quantization table is divided by 2 and middle part of the quantization table values is modified to one. The middle frequency area is utilized to embed two LSB of secrete message bits replaced with LSB of quantized DCT coefficients. This method achieves larger embedding capacity than Jsteg method and maintains similar image quality of Jsteg method while maintaining the compression ratio. Our proposed method uses this middle frequency data hiding approach for control experiment and additionally concentrates data hiding in some selected locations of lower frequency area to improve the embedding capacity with minimizing distortion in stego image and compression ratio is not affected in our approach as no changes made in higher frequency components.

Tseng and Chang proposed a quantization table based method in to maintain the balance between the embedding capacity, embedding rate and stego image quality [69]. The lower scaling factor and higher scaling factor are used in JPEG compression process and then quantization error is calculated to form a quantization error table. From this quantization error table, the DCT coefficients which are planned to zero after the quantization process are selected for data hiding. The embedding capacity of this method was increased as compared to Jsteg, F5 and Outguess in terms of quantization. Our proposed method is working similar to Tseng and Chang method in terms of different quantizer. In proposed method, some certain parts are modified (lower and middle frequency area) and remaining values are the same as original table.

The JPEG and Particle Swarm Optimization (PSO) based steganographic method was proposed by Li and Wang [106]. This method increases the embedding capacity than JMQT method in [79]. The stego image quality is kept by applying PSO algorithm. The produced optimal substitution matrix is used to embed the secrete message in quantized DC to middle frequency coefficients in each block. The embedding capacity of this method is larger than the JMQT method and the quality of stego images have good quality (based on larger PSNR) than JMQT method. The computational time and resultant image (stego image) size are the problems occurred in this method compared with JMQT. Similar to this method, our approach uses the AC coefficients in lower and middle frequency area by modifying lower part of the quantization table with different quantizer and middle part of the quantization table by one as stated in JMQT.

Adel Almohammad et.al proposed a novel JPEG steganographic method based on quantization table modification for gray cover images [77]. The image blocks are divided by 16×16 pixels and transformed by DCT to quantize by 16×16 quantization table derived from Chang et.al scheme [79]. The middle frequency area coefficients are utilized to hide two secrete message bits in order to improve the embedding capacity. The experimental results showed that the proposed method can embed more bits and stego images produced in this method is identical to cover image rather than Jsteg and Chang et.al's scheme [78].

Further, Adel Almohammad et.al extended his scheme to propose a hybrid method [107] that incorporates the proposed method with his previous scheme and Jsteg method. The aim of their method is to investigate the larger size of quantization table in JPEG steganography. The 16 x 16 quantization table is generated from standard quantization table used in JPEG compression scheme and it is optimized using optimization strategy proposed. JMQT method is applied to middle frequency coefficients while Jsteg method is applied to lower frequency area (14 quantized

DCT coefficients except DC coefficient in top left part of each block). The embedding capacity is considerably increased compared with Jsteg and JQMT but the quality of stego image is similar to JQMT and better than Jsteg. However, the optimization strategy is still challenge to modify the 16 x 16 quantization table.

Another 16×16 quantization table based JPEG steganography method was designed by Cuiling Jiang to improve the steganographic capacity and stego image quality [108]. All the lower and middle part of the quantization table values is changed to one except first element in the table to embed secrete message bits. This method is theoretically and experimentally analyzed and it show the high embedding capacity and good stego image quality compared with Chang et.al scheme [79] and Jsteg [78].

Brabin, D.R.D et.al proposed a data hiding method to hide secrete message in JPEG compressed images based on Quantization Error Table (QET) values which is generated by applying default quantization table and modified quantization table in compressed domain [109]. The higher frequency areas coefficients are used to hide secrete message bits in zigzag order. QET is applied to select the location among 26th position to 63rd position in image block for data embedding.

Cuiling Jiang et.al proposed a high embedding capacity JPEG steganography method [110] that incorporates F5 [103] and quantization table modification techniques [79]. Their method improve the embedding strategy to ignore the shrinkage produced by using F5 algorithm and also the experimental results has higher embedding capacity and better stego image quality in terms of PSNR.

Iwata et.al found that the AC coefficients after quantization step tend to be zero in the JPEG compression process and proposed a data hiding method that hides secrete message bits into higher frequency coefficients by using the length of the zero sequences among the quantized DCT coefficients [111]. This scheme uses the limits between the zero and non-zero coefficients to embed data.

Chang et.al extended Iwata et.al scheme to present lossless or reversible JPEG steganographic scheme for embedding secrete message in each block of quantized DCT coefficients [112]. The two successive zero coefficients of the medium frequency coefficients in each block are selected to embed secret data bits. In addition, the quantization table is modified to keep the imperceptibility of stego image while hiding large payload compared with Iwata et.al scheme.

An adaptive and reversible DCT based data hiding method was proposed by Lin et.al and it embeds secrete message bits into middle frequency of the quantized DCT coefficients and also it restricts the amount of non-zero values of the quantized DCT coefficients to participate in data hiding process [113].

Lin and Shiu proposed a method combined with Chang et.al scheme [114] to provide two layer data hiding scheme for JPEG images proposed in [112]. It achieves the reversibility but embedding capacity is restricted compared with Chang et.al scheme.

Hsien-Wen et.al proposed a high embedding capacity data hiding method for JPEG compressed images [115]. The suggested method derives capacity table to find the number of bits that can be embedded in quantized DCT coefficients to minimize the distortion produced in stego image. The default quantization table is used as threshold values to derive the capacity table based on human visual system. It was investigated with modified quantization table used in Chant et.al scheme and it achieves impressively larger embedding capacity than Chant et.al scheme [79].

Kan Wang et.al proposed a high-embedding capacity reversible data hiding scheme in JPEG-compressed domain [116]. It focuses on the modification of quantization table and quantized DCT coefficients. They choose selected elements in the upper left corner of the quantization table to be divided by an integer value whereas the equivalent quantized DCT coefficients are selected to be multiplied by the same integer value and adjusted to add a value to facilitate the high data embedding. This method analysis how some selected single quantized DCT coefficient in lower frequency area impact on the image quality by using PSNR, MSE and embedding capacity at quality level 70 and 90. The pros of this approach is that hiding order in lower frequency area is selected with the intention of helping to manage the enlargement of cover file size after embedding while keeping the PSNR value between the cover and stego-image is good with high embedding capacity in the meantime reversibility is achieved that the secrete message is extracted precisely and original JPEG cover can be restored. This approach will lead Chang et al.’s method [108] and Xuan et al.’s method [106] in terms of embedding capacity, image quality and file size. The proposed scheme is very practical for image files stored and transmitted in the JPEG format

Mohamad Amin et.al proposed a DCT based data hiding method [117]. It uses a mathematical operation to quantize the DCT coefficients then embeds the secrete message bits in all frequency coefficients in each block using LSB method. The experimental results shows the satisfactory results compared to Chang et.al scheme [41].

The quantization table is used to encode the DCT transformed coefficients to prepare for data hiding generated by a quality factor. The variation of quantization tables determines the embedding capacity of secrete message in terms of maintaining image quality. Po-Yueh Chen and Wei-Chih Chen proposed a quantization table based JPEG steganographic method based on the variation of quantization tables [75]. They used two scaling factor to modify quantization table to achieve correct extraction of secrete message and image quality respectively. The experimental results show the good PSNR values in terms of image quality.

A steganography method in JPEG compressed domain was proposed to show how a quantization table values are adjusted to provide space for data hiding in double compression effect [76]. It uses some permutation algorithm for data hiding in quantized DCT coefficients. The two different quality factors that are determined based on the binary value of secret message are dare applied to some region of the image to facilitate data hiding with. It provides more security and robust against attacks.

JPEG steganography raises the questions with the intention of image steganography requirements in the literature. The possibility of avoiding detection of secrete communication inside the stego image by third parties is questioned on insignificant statistical features of the DCT coefficients without giving up half size of embedding capacity. The second question is asking the maximum secrete message size that can be hidden in a given cover image without detecting the secrete communication in stego image. Third questions are related to the procedure that can achieve maximum embedding capacity. To answer these questions raised in literature, the solution is provided by modeling of cover image features lead to model based image steganography. The process of JPEG steganography compress the cover image by using quantization process and after this process, the secrete data is hidden before applying entropy encoding process as entropy encoding is lossless. In our approach, the double compressed image is provisionally converted to spatial domain and applies modified quantization tables to compress the image again with enabling the data hiding. This proposed technique works with lower frequency area data hiding for gray images. By combing experiments, for an image, we find the modified quantization table with relevant hiding pattern by combining four quantization tables with fifteen data hiding patterns. The joint statistical features that include DCT features of lower frequency area and some statistical features of spatial domain are extracted and experimentally investigated with the quantization table and data hiding pattern by using statistical analysis software to identify the correlation between them. Some positive correlation values found among the several combination of testing. Those correlated features are used to fit a model. According to passive warden scenario, this model based steganography is working. That is reduce the suspicion of secrete communication by attackers. According to correlated features of cover image, this proposed model is used to select the maximum message size to hide in cover image without degrading the image quality. The detailed description of proposed model based steganography for JPEG images will be discussed in chapter 3.

2.3 Summary

In this chapter, the issues concerning with DCT based data hiding and the role of quantization table in JPEG steganography process are carefully studied. Eventually, the fruitful argument is motivated for quantization table modification in JPEG steganographic process to satisfy the image steganographic requirements. Further, the features of our proposed method are conceptually compared with available relevant methods related to quantization table modification.

CHAPTER 3
JPEG STEGANOGRAPHY BASED ON QUANTIZATION TABLE MODIFICATION

3.1. Role of quantization table in JPEG steganography

In the process of JPEG encoding, quantization tables have a primary impact on the compression ratio and quality of compressed image with single quantization table or reconstructed image with double quantization table. It is obviously allowed to design or modify quantization table values in order to control the quality and compression ratio of resultant image [97]. Therefore, the generation of quantization table values is depend on the application such as JPEG steganography in order to meet the steganographic requirements. As mentioned in the chapter 1, the JPEG compression process is divided into lossless and lossy stages in terms of applying steganographic method. The quantization phase is lossy while Huffman encoding is lossless stage. The data hiding is not employed during the lossy stage since the redundant information is removed in this stage. However, the steganography process can take place in between the lossy and lossless stage. Actually, the quantized DCT coefficients are replaced with secrete message bits before entropy encoding stage in the JPEG process. The quantization table used in the steganography process provides space for data embedding in order to maintain the imperceptibility and image quality. The design or modification of quantization table values should be optimized to make steganographic system efficient. Therefore, applying optimized quantization tables with the steganography may improve the stego image quality and embedding capacity. Some of the methods related to quantization table modification were reviewed in the literature and the problem is identified among those methods. Finally, we have proposed a practical method to investigate the quantization table modification for a set of gray images in terms of applying steganography to satisfy the steganographic requirements and find the relationship between the quantization table modification, data hiding pattern and image features. This system allows users to freely select the modified quantization table against the best hiding pattern to achieve the high imperceptibility and high embedding capacity.

3.2. Mathematical description of JPEG steganography

As outlined the process of JPEG steganography in the chapter 1 in Figure 1.4 , the image representation in each 8 × 8 pixels blocks are transformed by 2D DCT which generates 64 DCT coefficients including one DC and 63 AC coefficients which are slightly different based on the human visual system in each block. These coefficients are then quantized by scalar quantizer specified by an 8 × 8 quantization table. The design of quantization table is based on the visual response to luminance variations on the intensity values, thus, a small variation among the intensity values is more visible in different frequency regions. The quantized coefficients are used to embed secrete message bits and lossless compression by arranging in zigzag manner.

Let I (x, y) denotes an 8-bit gray image with $x = 1, 2, \ldots.., M$ and $y = 1, 2, \ldots, N$. The $M \times N$ cover-image is partitioned into 8 × 8 blocks and each block is transformed by 2-D DCT.

Then the number of blocks L is depicted in the Equation 3.1.

$$L = (M \times N)/64 \tag{3.1}$$

Each block contains 64 pixels values.

The mathematical definition of DCT and IDCT is depicted in the Equations 3.2 & 3.3 [62].

Forward DCT

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=0}^{7}\sum_{j=0}^{7} f(i,j)\cos\left[\frac{\pi(2i+1)u}{16}\right]\cos\left[\frac{\pi(2j+1)v}{16}\right] \tag{3.2}$$

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} & for\ k = o \\ 1 & otherwise \end{cases} \tag{3.3}$$

Inverse DCT

$$f(i,j) = \frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7} C(u)C(v)F(u,v)cos\left[\frac{\pi(2i+1)u}{16}\right]cos\left[\frac{\pi(2j+1)v}{16}\right] \tag{3.4}$$

Here, *F (u, v)* and *f (i, j)* represent a DCT coefficient at the *(u, v)* coordinate and a pixel value at the *(i,j)* coordinate in image block, respectively.

F(0,0) is the DC component, which corresponds to an average intensity value of each block in the spatial domain. *F(u,v)* is the AC component in which u≠0 and v≠0. For data reduction during the quantization phase, DCT coefficients are quantized by using the standard quantization table shown in Figure 3.1.

The DCT is applied for each block *B$_i$*, *i=0…., L*, the DCT coefficients matrix for each block *D(a, b)*,

$$D_i[a,b] = DCT(Bi[a,b]) \qquad (3.5)$$

Where *0≤ a, b≤7* and *B$_i$[a, b]* is a pixel value in Bi and i denotes the block index, i=1…L. L is number of blocks

The quantization process for each block is designed by entropy thresholding technique that represented as matrix, which scales the quantized values by a compression Quality Factor (**QF**) [74]. The standard luminance quantization table denoted as QST is generated by using QF = 50 displayed in Figure 3.1.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 3.1: Standard JPEG quantization table [48].

The quantization table is stored in the DQT (define quantization table) segment in the image header [73]. In this study, the proposed experiment is done with the MIT JPEG library gray images [61]. The quantization tables with different quality factors are generated by using the following equation 3.6 [80] in the JPEG process.

$$QG(i,j) = \begin{cases} \left(\frac{100-QF}{50}\right) QST(i,j); if\ QF > 50 \\ \left(\frac{50}{QF}\right) QST(i,j); otherwise \end{cases} \qquad (3.6)$$

Where the QG is the generated quantization table for *i=0...,7* and *j=0...,7*. And QST is the standard quantization table with respect to *i, j*.

To compress the image data, these coefficients are then quantized by using a quantization table with 64 entries. The standard quantization table is shown in Figure 3.1. The quantized DCT coefficients are all integers which are obtained by dividing each DCT coefficient by its corresponding value in the quantization table and rounding to the nearest integer. The quantized DCT coefficient in each block is denoted as *QD (a, b)* generated by using the following Equation 3.7.

$$QD(a,b) = Round\left(\frac{D(a,b)}{Q(a,b)}\right) \tag{3.7}$$

Where, 0≤a, b≤7

DC coefficient corresponds to the lowest frequency in an 8×8 block, which is the average value over the 64 pixels. Hence, hiding in DC coefficient causes the much more distortion. The remaining 63 AC coefficients are the suitable for data hiding in terms of image steganography requirements. They can be categorized into lower frequency area, middle frequency area and higher frequency area. The human vision system is much more sensitive to the values in low-frequency components than those in the higher frequencies. Thus, distortion in high-frequency components is visually acceptable and perceptible. The non-zero AC coefficients available in low and middle is achieved good visual quality. Therefore, the upper left values in the quantization table are small enough to avoid large alteration. In contrast, the lower right values in the table are large and can be altered.

However, the selected area in the AC coefficients is arranged in Zig-Zag manner and it is used to hide the message bits.

The secrete message *S* of size *m* is converted into one dimensional bits stream s.

$$S = \{s_0, s_1, s_2 \ldots\ldots\ldots., s_{m-1}\} \tag{3.8}$$

Where, s_i is 0 *or* 1.

The LSB of the selected quantized DCT coefficients in each 8 × 8 block is replaced with the most significant bit (MSB) of the secrete message bits. The LSB of the coefficient and MSB of the message vary based on the requirement of hiding algorithm.

Suppose that, the message to be embedded in the range of $t1<i<t2$, $t3<j<t4$ in the quantized DCT block. Here, it can be simply denoted as

$$(t2 - t1) * (t4 - t3) = m \tag{3.9}$$

For the LSB replacement in each block is depicted in the following algorithm.

LSB algorithm to embed secrete message

```
for i=t1 to t2
    for j = t3 to t4
        for r=0 to m-1
            $MSB(S) = s_r$
            If LSB(QD(i, j))=1 and MSB(S)=o then resultant R(i,j)=LSB(QD(i,j))-1
            If LSB(QD(i,j))=0 and MSB(S)=1 then resultant R(i,j)=LSB(QD(i,j))+1
            If LSB(QD(i,j))=MSB(S) then resultant R(i,j)=LSB(QD(i,j))
        End
    End
End
```

Where, LSB(QD(i,j) is the least significant bit of the binary form of quantized DCT coefficients located in *(i,j)* position in an image block, MSB(S) is the most significant unassigned bit of the binary form of secret message. *R (i,j)* is the resultant of the message replacement for a coefficient in the *(i,j)* position.

Because of the rounding loss, the quantization step is not lossless. The final data stored in the JPEG file are the quantized DCT coefficients, which are entropy coded and saved in the entropy-coded segment of the header JPEG file. The quantization table is stored in the DQT (define quantization table) segment of the header.

The decompression process works conversely with compression process. The compressed JPEG file is prepared to get quantized DCT coefficients in each block.

The quantized DCT coefficients are multiplied by the primary quantization table values which are stored in the DQT segment denoted as $QP(i,j)$, where $0 \leq i, j \leq 7$ to get restored DCT domain and Inverse DCT is applied to reconstruct image in pixel domain $\hat{I}(x, y)$. $\hat{I}$ will generally differ from the original block *I*.

LSB algorithm to extract the secrete message

Decode the stego JPEG image to get the quantization table and quantized DCT blocks *QD'*.

```
for i=t1 to t2
    for j = t3 to t4
        m1 = LSB(QD'(i, j))
        S.add(m1)
    end
end
```

3.3. Steganography in JPEG compressed images

In JPEG compressed images, steganography are applied by using double compression effect using quantization table modification. The primary quantization table (QP) used in JPEG file is modified or optimized to provide space for data hiding by satisfying image steganography requirements. The modified table is called as secondary quantization table (QS).

Let *J (x, y)* is a JPEG compressed image which has a primary quantization table (QP) stored in DQT and image is decompressed (entropy decoded) to get quantized DCT coefficients and then de-quantized by multiplying by primary quantization table to get original DCT coefficients. The image is transformed by IDCT to get pixel domain image $\widehat{J}$ which is differing from *J*.

To recompress the image $\hat{J}$ with hidden secrete message bits, the reconstructed image $\hat{J}$ in pixel domain is transformed by 2-D DCT to serve DCT coefficients and apply secondary quantization table (QS) to get quantized DCT coefficients, which are the candidates for data hiding.

From the literature, to discuss the data hiding in three different frequency areas in DCT domain stated in Figure1.5, the JPEG coefficients belonging to middle frequencies may result without degrading the image quality with higher embedding capacity while data hiding in lower frequencies may result in less distortion but the embedding capacity is restricted. In higher frequency area data hiding may increase the stego file size with less distortion as most of the higher frequency coefficients are changed to zero after quantization process before the data hiding stage [77]. The effect of data hiding in these coefficients may significantly change the statistical properties of stego image. However, the frequency selection is based on the statistical properties of DCT coefficients or quantization error which is created by quantization table modification. Data hiding in these three frequency areas, the modification of quantization table plays major role to determine the imperceptibility and embedding capacity in different quality factors. In this approach, it has been developed a practical method that investigates the quantization table modification technique to select the coefficients in lower frequency area by evaluating the image quality parameters.

3.4. Overview of the proposed method

Effective image steganographic techniques are required to hide large message size while avoiding visual or statistical distortions. The DCT based data hiding technique is the core of JPEG steganography. The DCT is fully reversible and DCT based techniques are more robust compared to spatial domain techniques [94]. JPEG steganography can be divided into three frequency bands for data hiding. Generally, middle frequencies are elected for data hiding by researches due to the low energy concentration is low in that frequency area and it is less sensitive for HVS**.** Some of the research studies have been done in higher frequencies and these studies suffer from compression ratio and stego file size. In lower frequency area data hiding techniques may result a challenge with respect to embedding capacity. The trade-off between imperceptibility and embedding capacity is a big challenge in lower frequency area data hiding. The data hiding techniques used in lower frequencies and middle frequencies are required to modify the quantization table to achieve the balance between imperceptibility and embedding capacity. The first and good reversible steganographic technique that modifies mid part of the quantization table values by one was proposed by Chang et.al [70] to hide secrete message bits. This method uses middle frequencies to replace with two least significant bits of secrete message. Most of research studies were done based on this method. Some of them modifies top left corner of the quantization table values in order to hide data in lower frequencies by investigating the statistical properties of DCT coefficients with quantization table modification effect. Some of them generates quantization error and determines the embedding capacity based on the quantization error in all frequencies. However, this study elicited the quantization table modification techniques have some problems in the literature.

Quantization modification technique may be differing based on the image. There is no general modification technique to hide data that means researchers choose some particular images to apply quantization table modification for data hiding. Most of the techniques focus the particular coefficients in lower frequencies and scale them to hide data by modifying the relevant quantization table entry. It fails to investigate the other coefficients to hide data and to increase the embedding capacity. Therefore this study suggests a practical method to investigate the quantization table entries in top left part of the used common quantization table with a specified quality factor to hide data in lower frequencies in order to compete with literature by satisfying image steganographic requirements. Especially, this study suggest a practical method which improves the embedding capacity with high imperceptibility in lower and middle frequencies by evaluating the image quality parameters and finally the study focused to find the relationship between the quantization table modification effect and statistical properties of image for a JPEG compressed image data set that compressed with common quantization table with a certain quality factor.

3.4.1. A practical JPEG steganography method based on quantization table modification

Let an Image denoted by J_i in image dataset. $i = 1, 2, 3\dots\dots n$. n is number of images

Let primary quantization table used in the image dataset is denoted by $QP(i,j)$ for $0\leq i ,j\leq 7$

This proposed method can be divided into two stages in order to embed secrete message bits.

Stage 1: Quantization table modification

Let primary quantization table $QP(i, j)$, $0 \leq i, j \leq 7$

According to the literature, the middle part of the quantization table entries are modified to one such that $QP(i ,j)$ = 1.

Procedure 1:

```
Begin
    For $i = 1$ to 8
        For $j = 6-i$ to $9-i$
            If ($j \leq 0$)
            $j = 1$;
            $QP(i, j) = 1$
        End for
    End for
End.
```

The following Figure 3.2 illustrates a sample output produced by above Procedure 1.

				1	1	1	1
			1	1	1	1	
		1	1	1	1		
	1	1	1	1			
1	1	1	1				
1	1	1					
1	1						
1							

Figure 3.2 Modification of middle elements in primary quantization table [89]

The top left part of the quantization table for hiding data in lower frequencies of DCT domain are investigated in the proposed methodology in order to compete the quality degradation of image in terms of data hiding.

QP_{11}	**QP_{12}**	**QP_{13}**	**QP_{14}**	1	1	1	1
QP_{21}	**QP_{22}**	**QP_{23}**	1	1	1	1	
QP_{31}	**QP_{32}**	1	1	1	1		
QP_{41}	1	1	1	1			
1	1	1	1				
1	1	1					
1	1						
1							

Figure 3.3: Indented modified elements in top left part of the primary quantization

The quantization entries are scaled by dividing less than one to preserve the image quality [80]. Here, we choose three factors less than one, *f1, f2* and *f3,* to divide the quantization table entries stated in the Figure 3.4 and the middle part of the quantization table entries are modified to one according to literature. The bottom left part of the quantization table is kept with the same value. *f1 = ¼, f2 = ½* and *f3 = ¾* are the factors to divide the entries in quantization table to generate secondary quantization table values $QS_k(i, j)$ in each attempt relevant to generate data hiding patterns.

Procedure 2:

```
1. Begin
2.   For w = 1 to 3
3.     For i = 1 to 4
4.       For j = 1 to 5-i
5.         $QS(i, j) = QP(i, j) \times f_w$
6. End
```

Stage 2: Generation of data hiding patterns in lower frequencies with respect to quantization table modification.

The middle frequencies are utilized to replace with two least significant bits of secrete message by modifying mid part of the quantization table values to one as in the Figure 3.2.

Among the lower frequencies stated in Figure 3.3, it is randomly generated data hiding patterns in left to right, top to bottom and diagonal basis. The two least significant bits of any lower frequency coefficient shows the significant change in the image quality from the experimental results. Hence, one bit is selected to hide data in lower frequencies to compete with the existing method based on PSNR.

The derived PSNR for standard pattern that hides data only two bits in the middle frequencies is denoted as $PSNR_i$, where $i = 1, 2, 3\ldots\ldots n$. n is number of images.

The data hiding patterns are generated by spreading one LSB bit replacement among the nine lower frequency AC coefficients *AC1, AC2, AC3, AC8, AC9, AC10, AC15, AC16, and AC21* as shown in the Figure 3.4.

DC	AC1	AC2	AC3	AC4	AC5	AC6	AC7
AC8	AC9	AC10	AC11	AC12	AC13	AC14	
AC15	AC16	AC17	AC18	AC19	AC20		
AC21	AC22	AC23	AC24	AC25			
AC26	AC27	AC28	AC29				
AC30	AC31	AC32					
AC33	AC34						
AC35							

Figure 3.4: Different coefficients specified in the proposed approach

3.4.2. Generation of fifteen patterns using PSNR

3.4.2.1. The general algorithm is depicted to elect patterns for the investigation.

Input: Cover image dataset, standard pattern P_s, randomly generated pattern P_g, primary quantization table used in cover image dataset *QP*, modified tables called as secondary quantization table QS_k, 1<=k<=4

Output: Generated pattern P_g is selected or not

Procedure 3:

```
1. For $image_i$ $i = 1, 2 \ldots\ldots n$
2.    For $QS_k$,   $1<=k<=4$
3.       For $P_g$,   $1<=g<=2$
4.          Hide and generate stego image dataset
5.          Calculate $PSNR_v$, $1 \le v \le kg$
```

```
        End For
    End For
Max($PSNR_v$)  $v=1……k_g$
Extract the pair ($QS_k$, $P_g$)      $k=1…4$  and $g=1, 2$
End For
For the pair $(QS_k, P_g)_i$      $1<=i<=n, 1<=k<=4, 1<=g<=2$
If number of pairs ($QS_k$, $P_2$) > number of patterns ($Qd$, $P_1$) Where $P_2=Pg$ and $P_1=Ps$, Pg generated pattern Ps standard pattern
    Pattern $P_g$ is selected
```

3.4.3. Proposed practical method to select the quantization table and relevant hiding pattern

Input: Image dataset J_i, $1\leq i\leq n$, n indicates number of images, secret message S and length of the message is m, secret key, Generated patterns P_g, $1\leq g\leq p$, p indicates number of patterns generated and modified quantization tables QS_k, $1\leq k\leq q$, q indicates number of secondary quantization tables used

Output: Stego dataset R, $R_i \in R$, $1\leq i\leq n$, best secondary quantization table and hiding pattern for an image R_i is (QS_k, P_g), $1\leq k\leq q$, $1\leq g\leq p$.

Step 1*: Extract the primary quantization table (QP) from JPEG compressed image dataset.*

Step 2: *Modify the primary quantization table QP and generate the q number of secondary quantization tables q, QS_k, $1\leq k\leq q$, based on procedure 1.*

Step 3: *Randomly generate the p number of hiding patterns $P_g \epsilon P$, which are generated from procedure 2, using secondary quantization tables, $1\leq g\leq p$.*

Step 4:

```
For $i = 1$ to $n$,
  For $k = 1$ to $q$,
      For $g = 1$ to $p$
      Generate $R_{ikg}$ ,
      Compute PSNR ($J_i$, $R_{ikg}$)
    End For
  End For
 Max (PSNR ($J_i$, for all $R_i$)
Return ($k$, $g$)
End For
```

Step 5:

The size of cover image J is $M \times N$ pixels and partition the cover image J into non-overlapping blocks L. Each B_i contains 8×8 pixels for $i=0.....L$.

Step 6:

Use *DCT* to transform each block B_i into *DCT* coefficient matrix F_i,

$$F_i = DCT\ (B_i) \tag{3.10}$$

Where $0<=a, b<=7$ and $B_i[a, b]$ is the pixel value in block B_i.

Step 7:

Use selected modified or secondary quantization table QS_k, $1 \leq k \leq q$, to quantize each F_i. The result can be represented as

$$QC_i[a, b] = round\ (F_i\ [a, b]/QS_k[a, b]) \tag{3.11}$$

Step 8:

The actual message S as shown in the above equation 3.8 is represented in binary form and also size of the message is m.

Step 9:

Choose the selected pattern in step 4 *for the given* J_i image to employ hiding into quantized DCT coefficients in each.

Step 10:

Apply JPEG entropy coding, which contains Huffman coding to compress each block and Collect the above results and generate a JPEG file that contains the quantization table QS_k, $1 \leq k \leq q$, and all the compressed data.

In the previous algorithm, the sender investigates the secondary quantization tables with randomly generated hiding patterns and selects the best quantization table and hiding pattern in order to satisfy the requirements of imperceptibility and embedding capacity based on the PSNR evaluation. Here the sender is capable of hiding data using the selected pair of quantization table and hiding pattern and share them with receiver as secrete key to extract the secrete message bits at the receiver side. Where the secrete key denotes the particular pattern.

3.4.3.1. Framework of proposed practical method

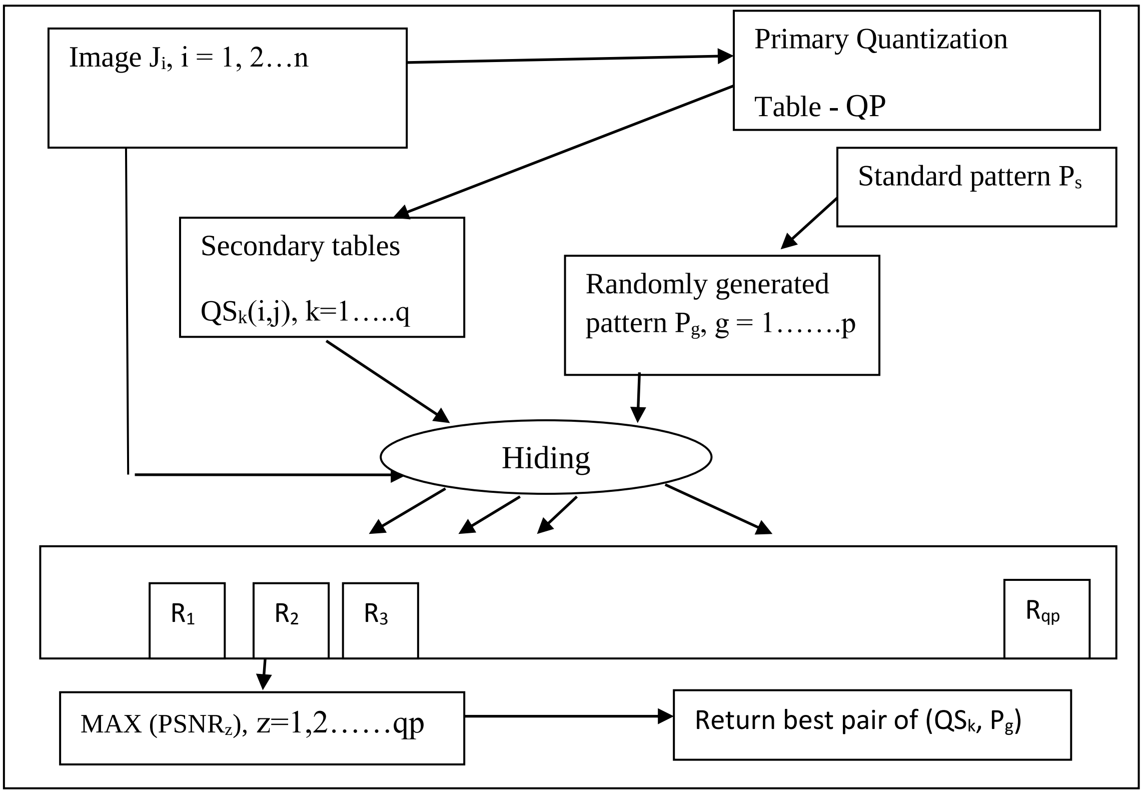


Image J_i, i = 1, 2…n
Primary Quantization Table - QP
Standard pattern P_s
Secondary tables $QS_k(i,j)$, k=1…..q
Randomly generated pattern P_g, g = 1…….p
Hiding
R_1
R_2
R_3
R_{qp}
MAX ($PSNR_z$), z=1,2……qp
Return best pair of (QS_k, P_g)

Figure 3.5: Block diagram of the proposed practical method

3.4.4. Extracting procedure

The receiver receives the double compressed JPEG image with secrete key that includes modified quantization table and hiding pattern. Receiver first decodes the image to get quantized DCT coefficients and extract the message by the secrete key shared by the sender.

3.4.5 Find the relationship between the cover image features, selected quantization table and hiding patterns

By the results of the above method given Figure 3.5, q secondary quantization tables are generated from primary quantization table and also it is investigated the randomly generated hiding patterns using these second quantization tables to hide secrete data by generating $q*p$ stego images per given image and found the best stego image based on the PSNR values. This methodology, finally, pave the path to extract the appropriate quantization table and data hiding pattern for a given image. Further, it has revealed a methodology to be investigated the cover image features with selected quantization table and hiding patterns. Each image has a pair that includes selected quantization table and hiding pattern.

Among the n number of images available in the image dataset, the pair of selected quantization table and hiding pattern may vary. By using a statistical model, we investigate to determine the correlation between the image features and other two dependent variables, quantization table QS_k and hiding pattern P_g by comparing p-value with each.

Analysis 1: (Image features, quantization table) – image feature is independent variable and quantization table is dependent variable.

Analysis 2: (Image features, hiding pattern) – image feature is independent variable and hiding pattern is dependent variable.

The significance level p-value is less than 0.05 indicates that the risk of concluding that a correlation exists.

3.4.5.1 Distribution of frequency coefficients in cover images

Our proposed practical method imposes the lower frequency data hiding that relates with nine AC coefficients in frequency domain. By hiding data, it affects the statistical properties of those AC coefficients, which may be changed or not. Hence, the statistical properties of those coefficients in lower frequencies should be investigated with respect to quantization table and hiding pattern. To do this, after applying DCT transformation on cover image dataset, the DC coefficients of all the blocks and the first nine AC coefficients (AC1, AC2 ….. AC9) in Figure 3.6 from the lower frequency area are selected in a left to right manner.

DC	AC1	AC2	AC3				
AC4	AC5	AC6					
AC7	AC8						
AC9							

Figure 3.6: DCT feature extraction in selected coefficients

3.4.5.2. Construct the distribution for DC and selected AC coefficients

The DC element in each block is generated to gather all DC coefficients in each block of the image in DCT domain such that:

$$D_{DC}= \{(b1)_{\mathrm{DC}}, (b2)_{\mathrm{DC}} \ldots.(bL)_{\mathrm{DC}}\} \qquad (3.12)$$

Where, $(bi)_{DC}$ indicates the frequency of DC coefficients in b_i block and L is the number of blocks.

The distribution of nine AC coefficients are formulated in the following equations such that :

$$D_{AC1}= \{(b1)_{\mathrm{AC1}},\ (b2)_{\mathrm{AC1}} \ldots (bL)_{\mathrm{AC1}}\} \qquad (3.13)$$

$$D_{AC2}= \{(b1)_{\mathrm{AC2}},\ (b2)_{\mathrm{AC2}} \ldots (bL)_{\mathrm{AC2}}\} \qquad (3.14)$$

$$D_{AC3}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC3}} \ldots (bL)_{\mathrm{AC3}}\}\} \qquad (3.15)$$

$$D_{AC4}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC4}} \ldots (bL)_{\mathrm{AC4}}\} \qquad (3.16)$$

$$D_{AC5}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC5}} \ldots (bL)_{\mathrm{AC5}}\}\} \qquad (3.17)$$

$$D_{AC6}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC6}} \ldots (bL)_{\mathrm{AC6}}\}\} \qquad (3.18)$$

$$D_{AC7}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC7}} \ldots (bL)_{\mathrm{AC7}}\} \qquad (3.19)$$

$$D_{AC8}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC8}} \ldots (bL)_{\mathrm{AC8}}\} \qquad (3.20)$$

$$D_{AC9}= \{(b1)_{\mathrm{AC3}},\ (b2)_{\mathrm{AC9}} \ldots (bL)_{\mathrm{AC9}}\}\} \qquad (3.21)$$

Where, (b1)*AC1*, (b2)AC2 .... (bL)AC9 are the frequencies of the AC1, AC2 ....AC9 coefficients in b_i block.

3.4.5.3. Feature extraction from cover images

In this research, the statistical features of distribution of lower frequency coefficients are also considered to investigate the effect of data hiding related to quantization table modification and data hiding patterns.

The statistical features, mean, standard deviation, skewness, kurtosis, energy and entropy of the distribution of the lower frequency DCT elements in each block are considered.

A discrete random variable *X*, with possible states x_1,x_2.....x_n.

The statistical feature mean is defined [37]. It can be calculated as:

$$Mean = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{3.22}$$

The statistical feature standard deviation is represented [37]. It can be defined as:

$$Std = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\mu)^2}{n}} \tag{3.23}$$

The energy measures the uniformity of the intensity level distribution. If the calculated energy value is high, the distribution indicates a small number of intensity levels [37] [99].

$$Energy = \sum_{i=1}^{n}[p(x_i)]^2 \tag{3.24}$$

The entropy measures the randomness of the distribution of the coefficients values over the intensity levels. If the entropy is high, then the distribution is among more intensity levels in the image. This is inverse of energy. A simple image has low entropy while a complex image has high entropy [37]. Entropy can be defined as:

$$Entropy = -\sum_{i=1}^{n} p(x_i) log_2 p(x_i) \tag{3.25}$$

The skewness is calculated for univariate data is in the Equation

$$Skew = \frac{\sum_{i=1}^{n}(x_i-\mu)^3/n}{\sigma^3} \tag{3.26}$$

Where, μ is the mean and σ is the standard deviation and n is the number of data points.

The kurtosis is calculated for univariate data is in the Equation

$$Kurtosis = \frac{\sum_{i=1}^{n}(x_i-\mu)^4/n}{\sigma^4} \tag{3.27}$$

Where, μ is the mean and σ is the standard deviation and n is the number of data points.

3.4.6. Correlation between image features, quantization table and hiding pattern

Let spatial features denoted as SP_f, DCT features denoted as DCT_f, Qk is secondary quantization table and P is a hiding pattern. To investigate the correlation, it is modeled as in R library.

$$(DCT_f \sim QS_k)\ ,\ 1 \leq k \leq q \tag{3.28}$$

Where image features are independent variable and quantization table is dependent variable.

$$(DCT_f \sim P_{g)},\ 1 \leq g \leq p \tag{3.29}$$

Where image features are independent variable and data hiding pattern is dependent variable.

3.4.7. Identification of quantization table and data hiding patterns using Model

In image steganography, cover selection plays major role to embed secrete message by investigating the statistical features of cover and stego images [73].

Some of the researchers did some experiments to investigate the efficiency of existing steganography methods for cover samples [17] [74].

The quantization table modification or optimizing quantization table based research studies in JPEG steganography suffers from investigation of set of coefficients with more possibilities of data hiding locations.

In this proposed approach, it is created a problem to increase the chances of modification of quantization table with existing quality factor and those modifications are investigated with more possibilities of data hiding patterns to find best quantization table and hiding pattern among the dynamically created quantization tables and hiding patterns. This is a dynamically adapted practical method for an image dataset.

The quantization table modification values and hiding locations are the parameters passed to this method.

Finally, it is intended to find the relationship between these parameters and image features.

3.4.7.1. Dynamic Model

This section is to investigate the significance relationship between the quantization table, data hiding pattern and image contents by generating dynamic model using statistical software. A simple classification frame work is provided to distinguish the variation of quantization tables (q) and data hiding patterns (p) with regarding to the extracted features of DCT coefficients for image set using statistical software.

Step 1: Collect the cover image samples n with the size of M×N with selected quantization table (QS_k) and data hiding pattern (P_g) to construct the sample image data set. Where, 1<=k<=q, 1<=g<=p

Step 2: Extract the statistical features of lower frequency DCT coefficients of cover samples and construct the feature vector with specified classes. In case of quantization table q classes and hiding patterns p classes.

Step 3: Build an identification model for sample image dataset using R library.

Step 4: Define the Hypothesis with assumption.

4.1: Analysis of quantization table
H0: There is no relationship between F_v and QS_k such that ($d \neq 0$), 1<=k<=q
H1: There is a relationship between F_v and QS_k

4.2: Analysis of data hiding pattern with
H0: There is no relationship between F_v and P_g such that ($d \neq 0$), 1<=g<=p
H1: There is a relationship between F_v and P_g

Where, d_{ij} refers the distance between the vectors z_i and z_j in the n×h data matrix and it can be calculated in the equation

$$d = \left[\left(z_i - z_j\right)^T \left(z_i - z_j\right)\right]^{1/2} \tag{3.30}$$

n is the number of images and h is the size of the feature vector. z_i and z_j are the raw vectors. F_v is the feature vector.
P-Value < 0.05, reject the Ho.

Step 5: Analyze the significance of the generated model by inspecting p-value.

3.4.7.2 Feature extraction in DCT domain

The feature vector is constructed by appending the statistical features of the lower frequency DCT coefficients in the Equation 3.27.

$$Fv = \{mean, std\text{-}dev, kurtosis, energy, entropy, skewness\} \qquad (3.31)$$

The statistical features, F_{VDC}, F_{VAC1}, F_{VAC2}, F_{VAC3}, F_{VAC4}, F_{VAC5}, F_{VAC6}, F_{VAC6}, F_{VAC7}, F_{VAC8}, and F_{VAC9} are calculated for the distribution of lower frequency coefficients, D_{DC}, D_{AC1}, D_{AC2}, D_{AC3}, D_{AC4}, D_{AC5}, D_{AC6}, D_{AC7}, D_{AC8}, and D_{AC9} respectively in image blocks.

$$FV = \{ F_{VDC}, F_{VAC1}, F_{VAC2}, F_{VAC3}, F_{VAC4}, F_{VAC5}, F_{VAC6}, F_{VAC6}, F_{VAC7}, F_{VAC8}, F_{VAC9}\} \qquad (3.32)$$

3.4.8. Dynamic model based JPEG steganography

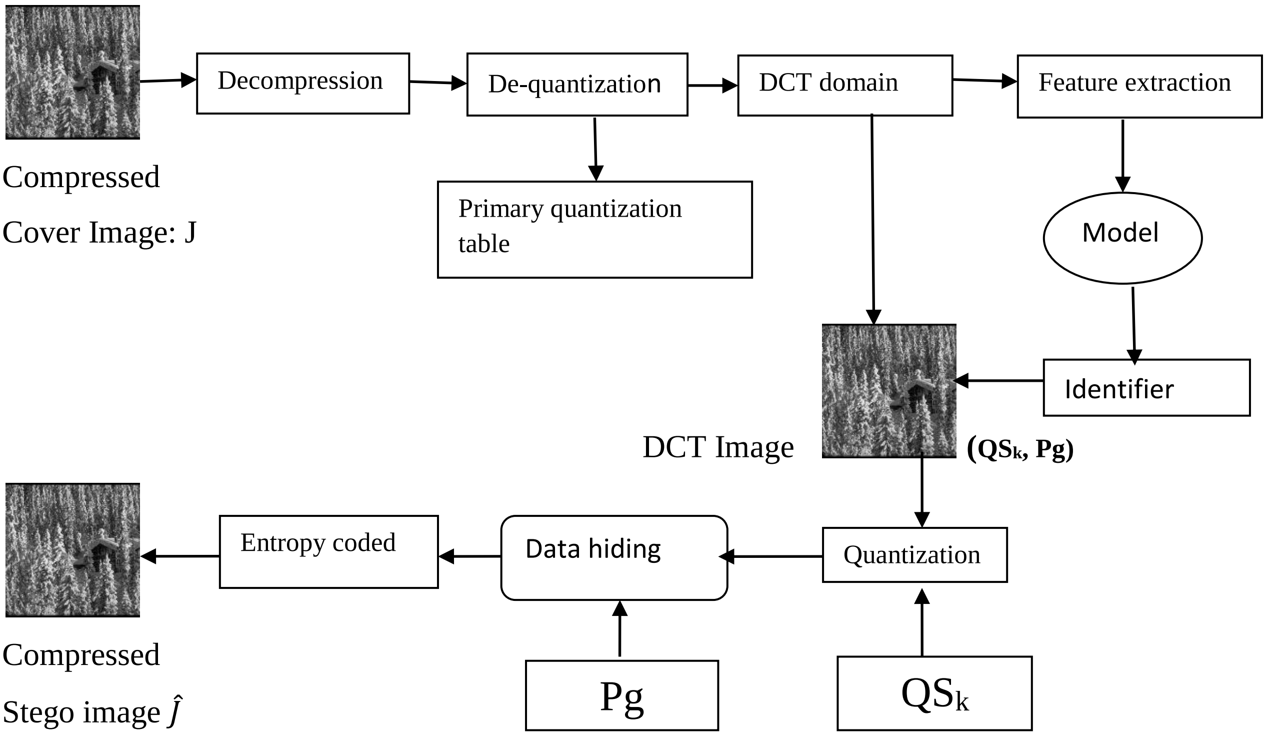


Figure 3.7: The proposed dynamic model based JPEG Steganography.

Procedure 4:

Step 1: Read JPEG compressed cover image *J*.

Step 2: Decompress the image and get quantized DCT coefficients in each block and extract primary quantization table. Let quantized coefficients *QD* and primary quantization table *QP*.

Step 3: De-quantize the quantized *DCT* coefficients by multiplying primary quantization table to get *DCT* coefficients.

$$DCT(a,b) = QD(a.b) \times QP(a,b) \qquad (3.33)$$

Step 4: Extract the DCT domain features and feed them into identification model to get modified quantization table QS_k and P_g hiding pattern. Where, 1≤k≤q and, 1≤g≤p, q indicates number of secondary quantization tables and p indicates number of generated patterns.

Step 5: Apply quantization to divide *DCT(a, b)* by QS_k and get quantized DCT coefficients *QD'(a,b)*.

Step 6: Apply received pattern P_j to hide data in lower and middle frequency elements to construct stego compressed image$\hat{J}$.

3.5. Chapter Summary

In our proposed approach, we present a practical method that dynamically adapt for JPEG compressed images. The cover image samples were compressed with same quantization table called primary quantization table. This is the motivation to choose the image dataset to propose this practical method. This method provides more possibilities for quantization table modification without considering the image quality. The image dataset maintains the same quality with the primary quantization table. Some top left part of the quantization table is divided by three different factors and middle part of the table entries are modified by one according to literature. The three different factors should always less than one in order to attain good image quality, imperceptibility and higher embedding capacity. The data hiding patterns are derived from the standard data hiding pattern by applying these modified quantization tables. Based on the PSNR results, the hiding pattern is selected. Finally, we create a combination of quantization tables and data hiding patterns to be investigated to find the best quantization table and hiding pattern for image dataset.

To prove the practical method, the statistical features are extracted from cover samples and correlated with quantization table and hiding pattern. Further, a model is created to discriminate the quantization table and hiding pattern against the image features. At the sender side, the model is used to extract the suitable quantization table and hiding pattern for an image and hiding will be continued after the prediction of modified quantization table and hiding pattern.

CHAPTER 4
EXPERIMENTAL SETUP

This chapter considers the experimental design of the proposed research work to investigate the impact of quantization table modification on the JPEG steganography. The experimental design in this chapter focuses to investigate the performance of the proposed JPEG steganography method. Thus, the experimental setup that combines quantization tables and data hiding patterns has been conducted in order to show the significance of quantization table modification reflected on embedding capacity, imperceptibility and image quality of resultant image for a specified image dataset.

The proposed method is coded in MATLAB R2015a and run on a Intel(R) Core(TM) i5 3210M CPU 2.50GHz (4CPUs), ~2.50GHz, Windows 7 Ultimate 32bit operating system.

4.1. Image set

The MIT Vision Tex image set consisting 328 JPEG compressed 256 × 256 size images are used as cover forest images displayed in Figure 4.1 for the experimental work. The sample images are high complexity and non-smooth area images that reduce the perceptual detection in terms of data hiding. Further, few images were used by the researchers in the literature to investigate the data hiding effect and shown the results. Hence, this image set is the nominated for this proposed study. The MIT Vision Tex forest images were compressed with same quantization table called primary quantization table in Figure 4.2 with a specified quality factor. The primary quantization table used in this image dataset is the key element to conduct the experiments and is first extracted from the image dataset to generate secondary quantization tables (QS_k) to investigate the impact of quantization table modification.

Figure 4.1: Sample Cover Images [61].

4.2. Quantization table modification

The proposed experimental setup is first to select an image from the cover image sample in Figure 4.1 in serial order and extract the primary quantization table in Figure 4.2 represented as matrix in MATLB.

8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	46	48	49	56	50	52	50

Figure 4.2: Extracted quantization table from cover image set

As stated in chapter 3, in the procedure 3.2, the following steps are carried out in order to modify the quantization table.

Step 1: Extract the primary quantization table from the image set stated in Figure 4.2.

Step 2: The middle part of the quantization table entries are modified by one as stated in Figure 4.3.

Step 3: The top left part of the primary quantization table is modified by multiplying three different factors f1 = 1/4, f2 = 1/2, and f3 = 3/4 to generate modified quantization tables (secondary quantization tables) displayed in Figure 4.4, Figure 4.5 and Figure 4.6 respectively. Each quantization table is represented as 2D matrix in MATLAB.

Step 4: Four modified quantization tables are generated by using the primary quantization table to conduct the experiments for cover image samples.

8	6	5	8	1	1	1	1
6	6	7	1	1	1	1	28
7	7	1	1	1	1	35	28
7	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Figure 4.3: Modified quantization table according to Literature

2	2	1	2	1	1	1	1
2	2	2	1	1	1	1	28
2	2	1	1	1	1	35	28
2	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Figure 4.4: (f1 = 1/4)

4	3	2	4	1	1	1	1
3	3	3	1	1	1	1	28
3	3	1	1	1	1	35	28
3	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Figure 4.5: (f2 = 1/2)

6	4	3	6	1	1	1	1
4	4	5	1	1	1	1	28
5	5	1	1	1	1	35	28
5	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Figure 4.6: (f3 = 3/4)

4.3. Data hiding pattern generation

The standard data hiding pattern in the literature depicted in Figure 4.7 were coded for the cover samples in MATLAB R2015a and we extract the PSNR values to evaluate the system.

				2	**2**	**2**	**2**
			2	**2**	**2**	**2**	
		2	**2**	**2**	**2**		
	2	**2**	**2**	**2**			
2	**2**	**2**	**2**				
2	**2**	**2**					
2	**2**						
2							

Figure 4.7: Number of bits to be hidden in middle frequency area [77] .

The data-hiding pattern is randomly generated in lower frequencies in left to right, top to bottom and diagonal basis by hiding one bit per DCT coefficient. The pattern generation method uses six parameters (4 modified quantization tables, standard hiding pattern and randomly generated pattern) to conduct the experiments to evaluate the performance of the randomly generated data hiding pattern based on the PSNR values. The significance of this method is that each data hiding pattern appends the embedding locations and embedding capacity.

The standard data hiding pattern and randomly generated hiding pattern are cross experimented with the generated four quantization tables. It will create eight (8) stego image samples for a cover image and the relevant PSNR values are extracted. The maximum PSNR value indicates the best quantization table and data hiding pattern for an image. This process is repeated for remaining cover samples. Each image has a best quantization table and data hiding pattern. The count of randomly generated data hiding pattern is more than standard hiding pattern, then we choose this randomly generated data hiding pattern is one of the parameters used in proposed methodology.

Pattern generation return the pair (QS_k,P_g) for $MAX\ (PSNR_w)$ for an image. Where, $1 \leq k \leq 4$, $1 \leq g \leq 2$, $1 \leq w \leq 8$. The fifteen patterns are randomly generated with comparing standard pattern by evaluating the relevant PSNR values. In the data hiding patterns, one and two represent the one bit hiding and two bits hiding in the specified location respectively while zero indicates the no hiding. The significance of generation of data hiding pattern in the proposed method covers the size of the message and location of embedding. Pattern 1 is generated from first diagonal positions except DC coefficient in lower frequencies as indicated in Figure 4.8.

0	1	0	0	2	2	2	2
1	0	0	2	2	2	2	
0	0	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.8: Pattern1

Pattern 2 is generated from second diagonal positions except DC coefficient in lower frequencies as indicated in Figure 4.9.

0	0	1	0	2	2	2	2
0	1	0	2	2	2	2	
1	0	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.9: Pattern 2

Pattern 3 is randomly generated from third diagonal positions except DC coefficient in lower frequencies as indicated in Figure 4.10.

0	0	0	1	2	2	2	2
0	0	1	2	2	2	2	
0	1	2	2	2	2		
1	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.10: Pattern 3

Pattern 4 is randomly generated from first row positions except DC coefficient in lower frequencies as indicated in Figure 4.11.

0	1	1	1	2	2	2	2
0	0	0	2	2	2	2	
0	0	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.11: Pattern 4

Pattern 5 is randomly generated from second row positions except DC coefficient in lower frequencies as indicated in Figure 4.12.

0	0	0	0	2	2	2	2
1	1	1	2	2	2	2	
0	0	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.12: Pattern 5

Pattern 6 is randomly generated from third row positions except DC coefficient in lower frequencies as indicated in Figure 4.13.

0	0	0	0	2	2	2	2
0	0	0	2	2	2	2	
1	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.13: Pattern 6

Pattern 7 is randomly generated from first column positions except DC coefficient in lower frequencies as indicated in Figure 4.14.

0	0	0	0	2	2	2	2
1	0	0	2	2	2	2	
1	0	2	2	2	2		
1	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.14: Pattern 7

Pattern 8 is randomly generated from second column positions except DC coefficient in lower frequencies as indicated in Figure 4.15.

0	1	0	0	2	2	2	2
0	1	0	2	2	2	2	
0	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.15: Pattern 8

Pattern 9 is randomly generated from third column positions except DC coefficient in lower frequencies as indicated in Figure 4.16.

0	0	1	0	2	2	2	2
0	0	1	2	2	2	2	
0	0	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.16: Pattern 9

Pattern 10 is randomly generated from second row and second column positions except DC coefficient in lower frequencies as indicated in Figure 4.17.

0	0	0	0	2	2	2	2
0	1	1	2	2	2	2	
0	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.17: Pattern 10

Pattern 11 is randomly generated from second and third columns positions except DC coefficient in lower frequencies as indicated in Figure 4.18.

0	1	1	0	2	2	2	2
0	1	1	2	2	2	2	
0	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.18: Pattern 11.

Pattern 12 is randomly generated from second and third rows positions except DC coefficient in lower frequencies as indicated in Figure 4.19.

0	0	0	0	2	2	2	2
1	1	1	2	2	2	2	
1	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.19: Pattern 12.

Pattern 13 is randomly generated from mixed diagonal positions except DC coefficient in lower frequencies as indicated in Figure 4.20.

0	0	0	1	2	2	2	2
0	1	1	2	2	2	2	
0	1	2	2	2	2		
1	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.20: Pattern 13.

Pattern 14 is randomly generated from mixed row and column positions except DC coefficient in lower frequencies as indicated in Figure 4.21.

0	1	0	0	2	2	2	2
1	1	1	2	2	2	2	
0	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.21: Pattern 14.

Pattern 15 is randomly generated from mixed diagonal positions except DC coefficient in lower frequencies as indicated in Figure 4.22.

0	0	1	0	2	2	2	2
0	1	1	2	2	2	2	
1	1	2	2	2	2		
0	2	2	2	2			
2	2	2	2				
2	2	2					
2	2						
2							

Figure 4.22: Pattern 15

4.4. Cross experiments combined quantization table and data hiding patterns

From the above experiments, the fifteen data hiding patterns employed in lower and middle frequencies are generated by investigating the four modified quantization tables for cover image samples. The fifteen data hiding patterns with these four modified quantization tables are the candidates to investigate the efficiency of data hiding in terms of embedding capacity, imperceptibility and image quality. The major experimental setup appends four modified quantization tables and fifteen data hiding patterns with secrete message bits. An image is cross experimented to hide secrete message with four modified quantization tables aligned with fifteen data hiding patterns and this setup creates sixty (60) stego samples for an image. In each stego sample, the PSNR is calculated and maximum PSNR value indicates relevant modified quantization table and suitable data hiding pattern as high PSNR value specifies high imperceptibility of stego image. Each generated patterns shows more embedding capacity than standard hiding pattern in Figure 4.7. Additionally, other requirements of image steganography, image quality and security that means undetectability of secrete message inside the stego image are investigated by testing the statistical image features of both cover and stego image. Our proposed methodology fully attends imperceptibility test by evaluating the PSNR since the image dataset relates with texture contents.

4.4.1. Experimental design of proposed approach

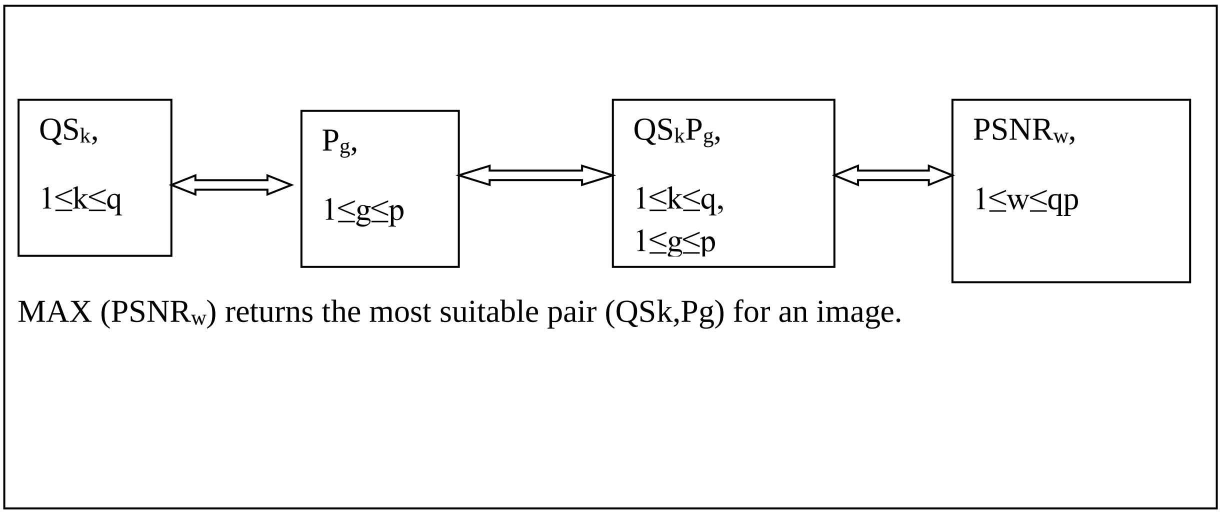

QS_k, $1 \leq k \leq q$
P_g, $1 \leq g \leq p$
QS_kP_g, $1 \leq k \leq q$, $1 \leq g \leq p$
$PSNR_w$, $1 \leq w \leq qp$
MAX ($PSNR_w$) returns the most suitable pair (QSk,Pg) for an image.

Figure 4.23: Block diagram of cross experiments with q quantization tables and p hiding patterns.

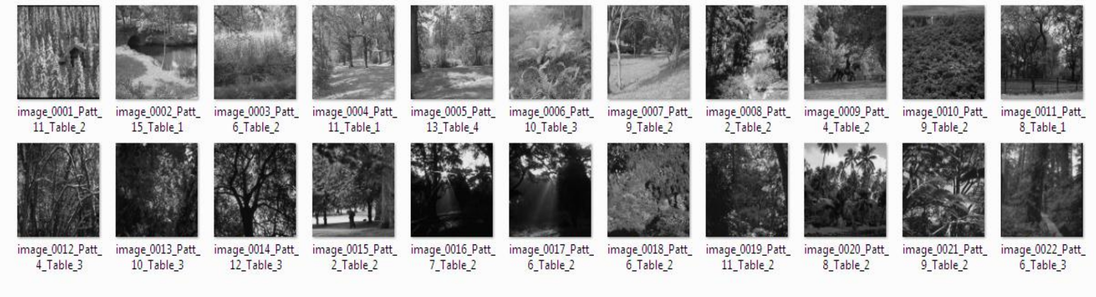


image_0001_Patt_11_Table_2
image_0002_Patt_15_Table_1
image_0003_Patt_6_Table_2
image_0004_Patt_11_Table_1
image_0005_Patt_13_Table_4
image_0006_Patt_10_Table_3
image_0007_Patt_9_Table_2
image_0008_Patt_2_Table_2
image_0009_Patt_4_Table_2
image_0010_Patt_9_Table_2
image_0011_Patt_8_Table_1
image_0012_Patt_4_Table_3
image_0013_Patt_10_Table_3
image_0014_Patt_12_Table_3
image_0015_Patt_2_Table_2
image_0016_Patt_7_Table_2
image_0017_Patt_6_Table_2
image_0018_Patt_6_Table_2
image_0019_Patt_11_Table_2
image_0020_Patt_8_Table_2
image_0021_Patt_9_Table_2
image_0022_Patt_6_Table_3

Figure 4.24: Sample stego images with respected to selected quantization table and hiding pattern.

4.5. Relationship between quantization table, data hiding pattern and image features

4.5.1. Feature Extraction

A JPEG compressed image with 256 × 256 size is first decompressed to get quantized DCT coefficients and then de-quantized with primary quantization table in Figure 4.2 to get DCT coefficients. After that, IDCT is applied to get image in spatial domain. The restored image is divided into 8 × 8 non-overlapping blocks.

The number of blocks are (256/8) × (256/8) = 1096 blocks

Each block is transformed by DCT and DCT domain features are extracted from the lower frequencies.

For each block, DC coefficient and nine AC coefficients are extracted and the histogram of each coefficient is produced. After that, we extract the statistical features of each histogram to investigate the relationship between quantization table and data hiding pattern.

The combination of extracted statistical features is the candidate to generate statistical model.

4.5.2. Find the correlation between the quantization table, data hiding pattern and image features using R library.

As mentioned in chapter 3, the extracted features are combined and mapped with quantization tables and data hiding patterns. In order to achieve this, the following steps are performed in the experimental step.

Step 1: Import the required data into R

Step 2: Visualize the imported data using R command.

Step 3: Make preliminary test to check the test assumptions.

Step 4: Initialize the Hypothesis with assumption.

Step 5: Use the ANOVA test for the imported data and find the P-Value

Step 6: Based on the P-Value < 0.05, the significance relationship between the image contents and parameters will be determined.

Step 7: Plot the equation for the relationship.

4.5.3 Identification of data hiding patterns and quantization tables with respect to image features by generating dynamic model

The proposed method generates dynamic models to identify the best quantization table and relevant data hiding pattern for cover image dataset by using the image features. It identifies a data hiding pattern that appends embedding location and embedding capacity for a cover image. Based on the extracted features from cover images, it is constructed dynamic model that is robustness to the image steganography system. The security of the system is achieved by generating the dynamic model. The proposed system is stego invariant for selected features. No one can detect the existence of the message without knowing the selected features. It achieves the robustness of the system.

4.6. Performance Evaluation Parameters

To investigate the performance of the proposed method, some performance evaluation parameters related to image steganography are implemented in MATLAB. Each compressed image in several occurrences is used to hide data to produce a set of stego images. To find a most suitable stego image among the set of stego images for a cover image, these performance evaluation parameters are used to make final judgment. Some of the following performance evaluation parameters are used in this experimental set.

4.6.1. The imperceptibility test

Steganography is a key contributor of information security. Information security achieves security through steganography by evaluating the imperceptibility of resultant media. The imperceptibility of stego image with respect to proper cover image plays fundamental role in image steganography. Usually, this is measured by PSNR as stated in chapter 1. The PSNR is implemented in MATLAB by considering the cover image and stego image. The actual cover image is read and applies data hiding to cover image to generate stego image. These two cover and stego images are the parameters for the PSNR calculation.

In the experimental setup, the calculated PSNR value indicates the level of imperceptibility and distortion of resultant image. The high PSNR values indicates high imperceptibility while low PSNR value shows the significance of changes in the stego images by hiding effect.

The heuristic values of PSNR are between 30dB and 50dB for image steganography in the literature [33]. Otherwise, the PSNR value is less than 30 indicate that the distortion is oblivious in stego image [58].

In our proposed approach, we use JPEG compressed images that appends texture contents. This will lead to high undetectability of existence of the secrete message inside the stego image.

4.6.2. The Image quality test

The mathematical relationship of image quality measure is expressed by the statistical evidence that can be calculated between the cover image and stego image. This measures the similarity between the cover and stego image. There are several image quality measures available in literature. Some of them are Normalized Correlation Coefficient (NCC), Structural Similarity Content (SCC), Absolute Difference value (AD) etc. Here, we investigate the Absolute Difference (AD) to evaluate the image quality. The AD value is closer to one, the higher level of similarity between cover and stego image is achieved [70].

The Normalized cross-correlation coefficient can be calculated by using the Equation 4.1.

$$Ncc = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)\times S(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j))^{2}} \qquad (4.1)$$

Where, *C (i,j)* is the Cover image and *S (i,j)* is its corresponding Stego image. $M\times N$ is also image file size.

Structural content (SC) is also correlation based measure and measures the similarity between two images and it can be calculated by using the Equation 4.2.

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{S}(\boldsymbol{i},\boldsymbol{j}))^{2}}{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{C}(\boldsymbol{i},\boldsymbol{j}))^{2}} \qquad (4.2)$$

4.6.3. The security of image steganography

The security of an image steganographic system can be evaluated away from assessing the distribution of the cover and stego image. The statistical measure of secure image steganographic system can be modeled as in the Equation 4.3.

$$RE(P_{C},P_{S}) = \sum P_{C}\left|log\frac{P_{C}}{P_{S}}\right| \qquad (4.3)$$

Where P_C and P_S indicate the distribution of cover and stego image and the relative entropy RE (P_C, P_S) is zero indicates that the image steganography system is perfect secure [54].

4.7 Chapter Summary

This chapter summarizes the design of experiments to implement the proposed methodology. An image steganographic system that contains the JPEG compressed images works with quantization table modification based data hiding. Some of the elements of the primary quantization table are modified without disturbing the image quality and also the data hiding patterns that append embedding locations and embedding capacity are generated randomly among the lower frequencies in order by using modified quantization tables and standard data hiding pattern. The proposed method finds most suitable modified quantization table for an image with higher embedding capacity. Further, a stego invariant model is proposed to classify the modified quantization table and data hiding pattern for an image based in the image features.

CHAPTER 5:
RESULTS AND DISCUSSION

This chapter elaborates the experimental results of the proposed JPEG steganography method and discusses the analysis to demonstrate the performance of the proposed lower frequencies data hiding method in terms of image steganography requirements such as imperceptibility, embedding capacity, image quality and security based on the extracted results. The experimental results focus on the measure of imperceptibility, embedding capacity and image quality in order to evaluate the proposed practical JPEG steganography method.

5.1. The PSNR of standard pattern

Each block in an image utilizes middle frequencies to hide two LSBs of quantized DCT coefficients replaced with MSB of secrete message bits [38]. The standard data-hiding pattern was coded with four modified quantization tables and the PSNR values for the image samples are displayed in the Figure 5.7.

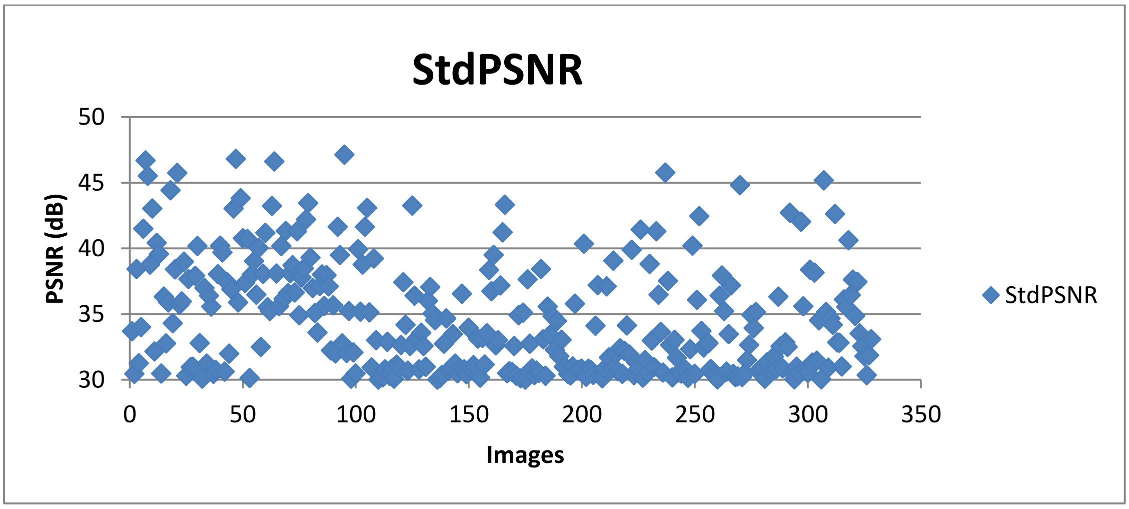


Figure 5.1: The PSNR values for standard hiding patterns with modified quantization tables

The scatter plot of PSNR values is the results of standard hiding pattern that replaces two LSBs of quantized DCT coefficients with MSB of secrete message bits. Since the cover images used in this experiment are JPEG compressed, this experiments show the double quantization process. Generally, the PSNR values for double quantization based steganographic techniques fall in the range of 30 to 40 and it is the good indication for imperceptibility of stego image in compressed domain [15].

The 328 JPEG compressed are used to hide data according to standard pattern by using four modified quantization tables. The first quantization table modification strategy is used according to the literature [68]. Other three modifications made in top left part of the quantization table only divide some elements of quantization table by different factors. Figure 5.1 depicts that the most of the images show the PSNR values between 30 to 45dB. In this study, it has been observed that the stego images which satisfy the PSNR values near 30 and those are less attention of traces produced by hiding effect since those images are mixed contents. Hence, the PSNR value 30 is a threshold level to hide maximum message size without causing distortion. Our proposed method competes with the standard data hiding method with 4 modified quantization tables with 15 generated hiding patterns to hide more data bits in lower frequencies more than PSNR values derived in Figure 5.1.

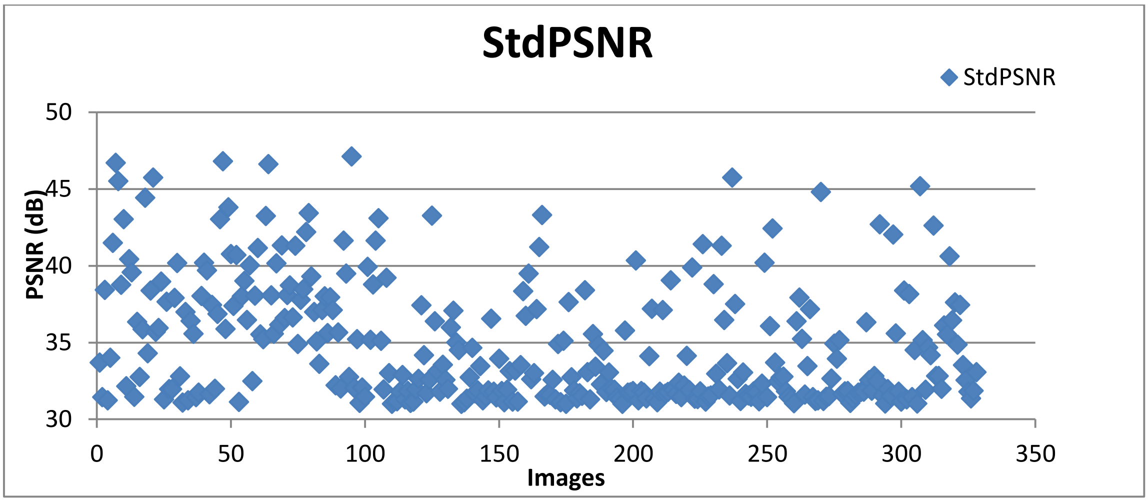


Figure 5.2: The PSNR values for standard hiding patterns with four modified quantization tables

This results show the valid reason for the need of quantization table modification. Among the 328 images, only 81 images satisfy with the first modified quantization table for standard data hiding pattern in Figure 4.7 and the remaining images need other modified quantization table for standard data hiding pattern. This obviously states that the modification in top left part of the quantization table will show the higher PSNR values for middle frequency data hiding.

The derived PSNR values in the Figure 5.1 is the initial results of our proposed method and it is used to generate data hiding patterns in lower frequencies by comparing the generated PSNR values in displayed in Figure 5.2 with four modified quantization tables.

Table 5.1: Number of selected secondary quantization tables for the image set

Modified Quantization Table QS_K	Number of QS_k for selected for stego images based on PSNR
Q1	81
Q2(f1 = 1/4)	72
Q3(f2 = 1/2)	98
Q4(f3 = 3/4)	77

5.2. Results and Analysis of data hiding patterns generation

5.2.1. PSNR analysis for Pattern 1

The standard hiding pattern and newly randomly generated data hiding pattern in lower frequencies were implemented with four modified quantization tables. The PSNR values for the pattern 1 were compared with the standard data hiding pattern. The 221 images show the higher PSNR values for the pattern 1 than the PSNR values for standard hiding pattern. The remaining 117 images keep standard pattern with PSNR values more than 30. Hence, the pattern 1 is selected to participate in this proposed practical method. The comparison of pattern 1 PSNR values with standard hiding pattern is illustrated in the Figure 5.3. The PSNR range falls in 30 to 45 for stego images that satisfy Pattern 1. This is the acceptable range for good imperceptibility for compressed images.

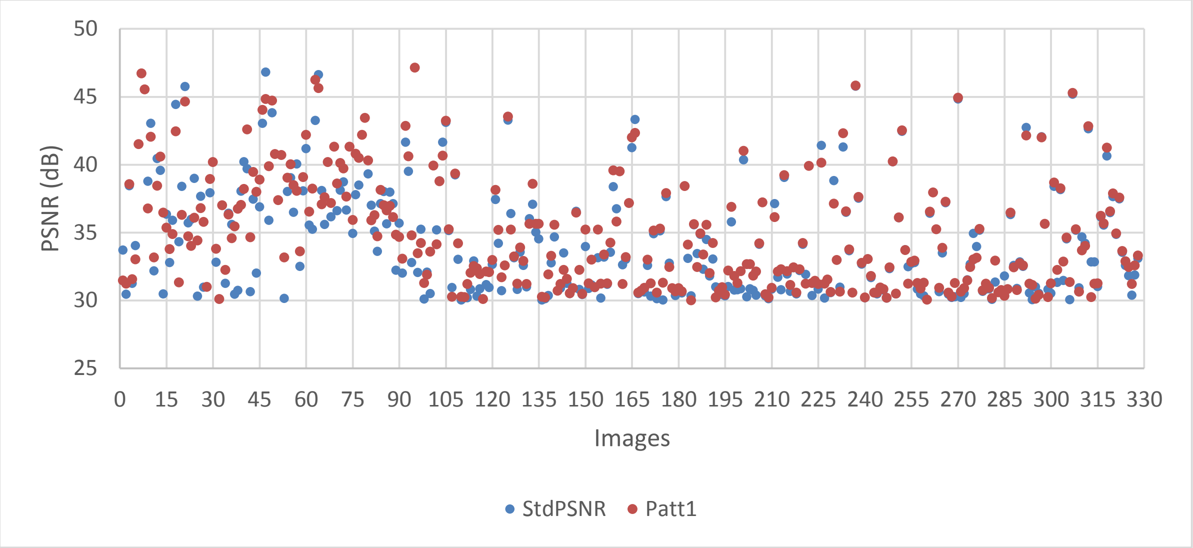


Figure 5.3: PSNR comparison of Standard hiding pattern and Patter 1 for image set.

Table 5.2: Statistical difference between the PSNR values

Regression Statistics					
Multiple R	0.957671115				
R Square	0.917133965				
Adjusted R Square	0.916879775				
Standard Error	1.185383893				
Observations	328				
ANOVA					
	df	*SS*	*MS*	*F*	*P-Value*
Regression	1	5069.812	5069.812	3608.061	2.2858E-178
Residual	326	458.074	1.405135		
Total	327	5527.886			

In the Table 5.2, the summary of regression statistics is depicted. The ingredients of regression statistics such as Multiple R, R Square, adjusted R Square and Standard Error values indicate the goodness-of-fit measures of the PSNR values of the standard hiding method and pattern 1 hiding method. The Multiple R value and R Square values shows the 95.76% and 91.71% of the variation between the standard PSNR values and the proposed PSNR values. Further, ANOVA test with four values such as df (degrees of freedom), SS (Sum of Squares), MS (Mean Squares), F ratio and P-Value show the values in terms of regression analysis. The P-Value in the analysis (2.2858E-178 < 0.05) indicates the good significance between both PSNR values. $R^2 = 0.9171$ means that 91.71% of the variation of Patt1PSNR by the regress of StdPSNR. A simple summary of the above output is that the fitted line in the equation 5.1.

$$Y = 2.6258 + 0.9343X \tag{5.1}$$

Y specifies Patt1PSNR, 2.6258 indicates the intercept and 0.9343 is the coefficient to regress the StdPSNR specified by X.

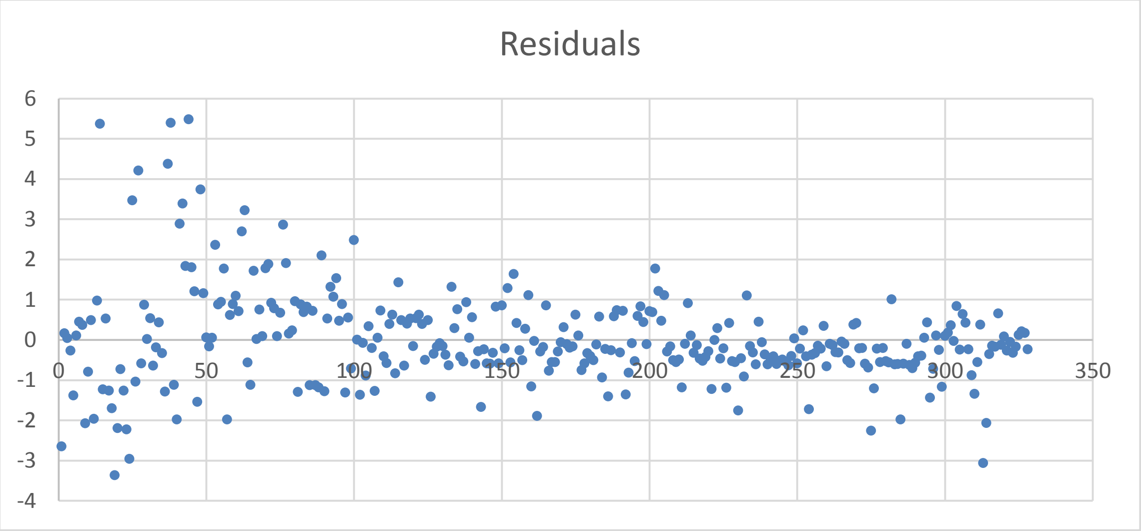


Figure 5.4: Residual plot of PSNR values for image set

This process is continued for the remaining randomly generated data hiding patterns in lower frequencies. Each randomly generated pattern is coded with standard pattern for 4 modified quantization tables. The PSNR values for both patterns are compared and discussed to make the judgment for selecting the randomly generated pattern to participate in this proposed practical method. Here, we show the results of remaining 14 randomly generated patterns in terms of PSNR values.

Table 5.3: The results of other patterns and their PSNR range

Pattern1	Standard Pattern	Pattern1
Number of patterns	117	221
PSNR range	30db-48db	30db-45db

Pattern 2	Standard Pattern	Pattern 2
Number of pattern	156	172
PSNR range	30db – 45db	31db – 41db
Pattern 3	Standard Pattern	Pattern 3
Number of pattern	170	158
PSNR range	30db – 45db	33db – 42db
Pattern 4	Standard Pattern	Pattern 4
Number of pattern	150	178
PSNR range	30db – 45db	31db – 40db
Pattern 5	Standard Pattern	Pattern 5
Number of pattern	152	176
PSNR range	30db – 45db	30db – 44db
Pattern 6	Standard Pattern	Pattern 6
Number of pattern	158	170
PSNR range	30db – 45db	31db – 45db
Pattern 7	Standard Pattern	Pattern 7
Number of pattern	166	162
PSNR range	30db – 45db	31db – 42db
Pattern 8	Standard Pattern	Pattern 8
Number of pattern	170	158
PSNR range	30db – 45db	30db – 40db
Pattern 9	Standard Pattern	Pattern 9
Number of pattern	177	151
PSNR range	30db – 45db	32db – 42db
Pattern 10	Standard Pattern	Pattern 10
Number of pattern	156	172

PSNR range	30db – 45db	31db – 44db
Pattern 11	Standard Pattern	Pattern 11
Number of pattern	158	170
PSNR range	30db – 45db	30db – 43db
Pattern 12	Standard Pattern	Pattern 12
Number of pattern	167	161
PSNR range	30db – 45db	30db – 42db
Pattern 13	Standard Pattern	Pattern 13
Number of pattern	151	177
PSNR range	30db – 45db	32db – 41db
Pattern 14	Standard Pattern	Pattern 14
Number of pattern	176	152
PSNR range	30db – 45db	31db – 44db
Pattern 15	Standard Pattern	Pattern 15
Number of pattern	157	171
PSNR range	30db – 45db	30db – 39db

5.3. The results and justification for proposed practical JPEG steganography method

From the pattern generation experimental results, based on the PSNR values, the randomly generated patterns were selected. More than 290 images needs data hiding in lower frequencies in the 15 pattern generation experiments. Few images do not change the standard hiding pattern. But, they show the little bit difference of PSNR values for the other generated patterns. Therefore, the generated hiding patterns compete with their PSNR values for image dataset. We investigate the competition of those generated patterns each other for image dataset and analyze the performance of the patterns in terms of imperceptibility, image quality and embedding capacity. The four modified quantization tables are cross checked with fifteen data hiding patterns. The 60 stego images are generated for an image in cover samples. Based on the maximizing PSNR, the suitable quantization table and relevant data hiding pattern is selected for an image. This experiment provides more chances to investigate the quantization table modification effect that reflects on location of embedding in lower frequencies. Imperceptibility and embedding capacity are the two important requirements considered in JPEG steganography. In our proposed method, the standard hiding pattern is appended with generated different patterns in lower frequencies. The data hiding pattern finds and locates the optimum secrete message bits without distorting the image that represents maximum PSNR value for stego image.

5.3.1 The performance of proposed method

The four quantization tables and fifteen data hiding patterns are the candidates of the proposed method and imperceptibility is a key factor that discriminates the data hiding method based on the performance of the PSNR values of relevant cover and stego images. The proposed method returns the quantization table and data hiding method based on the PSNR values. The calculated PSNR values for this proposed method is compared with the PSNR values for standard data hiding pattern in this section. The figures (Figure 5.5 to Figure 5.7) below indicate the PSNR values for proposed method. The comparison of both proposed and standard hiding method is illustrated in the Figure 5.1. The PSNR values for most of the images in the proposed method are significantly improve the PSNR values of the images in standard hiding pattern method and the PSNR values fall in the range of 31db to 43 db for the proposed method. The retrieved PSNR values for both are displayed in the Appendices.

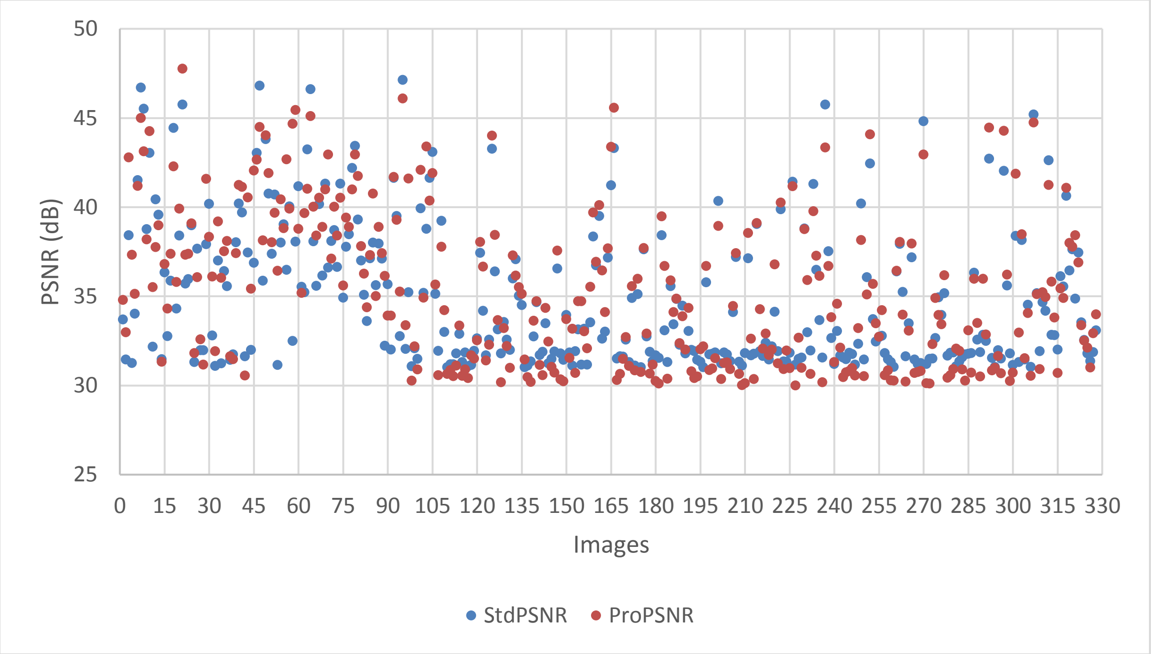


Figure 5.5: The comparison of PSNR values of proposed hiding method with standard hiding method for image set.

Table 5.4: Statistical difference between the PSNR values

Regression Statistics					
Multiple R	0.9115043				
R Square	0.83084				
Adjusted R Square	0.8303211				
Standard Error	1.7642873				
Observations	328				
ANOVA					
	df	*SS*	*MS*	*F*	*P-Value*
Regression	1	4983.977	4983.977	1601.17	7.8973E-128
Residual	326	1014.743	3.11271		
Total	327	5998.72			

In the Table 5.4, the summary of regression statistics is depicted. The ingredients of regression statistics such as Multiple R, R Square, adjusted R Square and Standard Error values indicate the goodness-of-fit measures of the PSNR values of the standard hiding method and proposed hiding method. The Multiple R value and R Square values shows the 91.15% and 83.08% of the variation between the standard

PSNR values and the proposed PSNR values. Further, ANOVA test with four values such as df (degrees of freedom), SS (Sum of Squares), MS (Mean Squares), F ratio and P-Value show the values in terms of regression analysis. The P-Value in the analysis (7.8973E-128 < 0.05) indicates the good significance between both PSNR values. $R^2 = 0.8308$ means that 83.08% of the variation of ProPSNR by the regress of StdPSNR. A simple summary of the above output is that the fitted line in the equation 5.2

$$Y = 0.6129 + 0.9941X \tag{5.2}$$

Y specifies ProPSNR, 0.6129 indicates the intercept and 0.9941 is the coefficient to regress the StdPSNR specified by X.

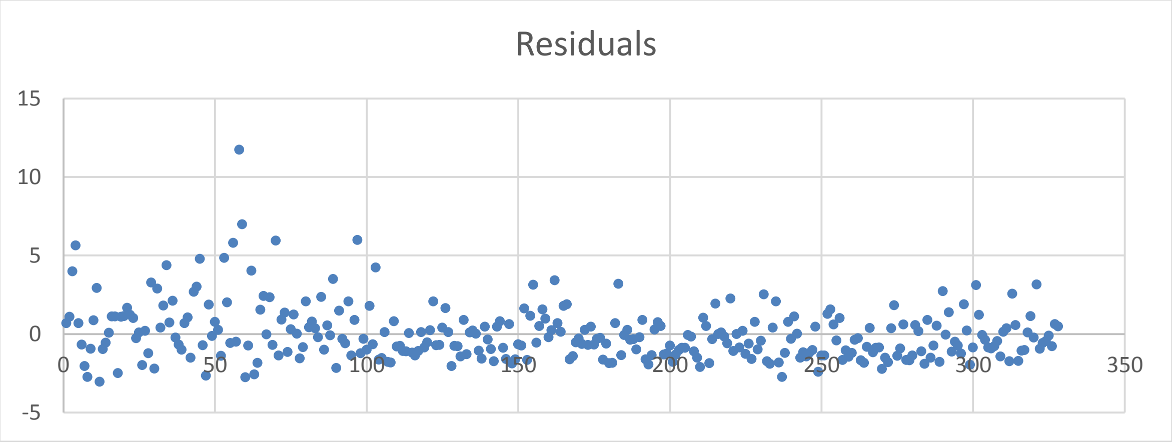


Figure 5.6: Residual plot of PSNR values for image set

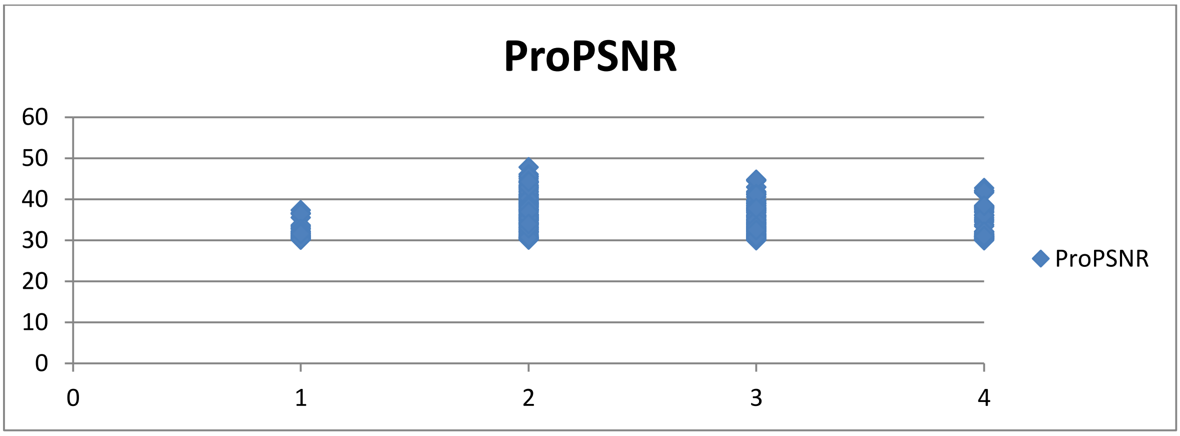


Figure 5.7: PSNR range for quantization tables

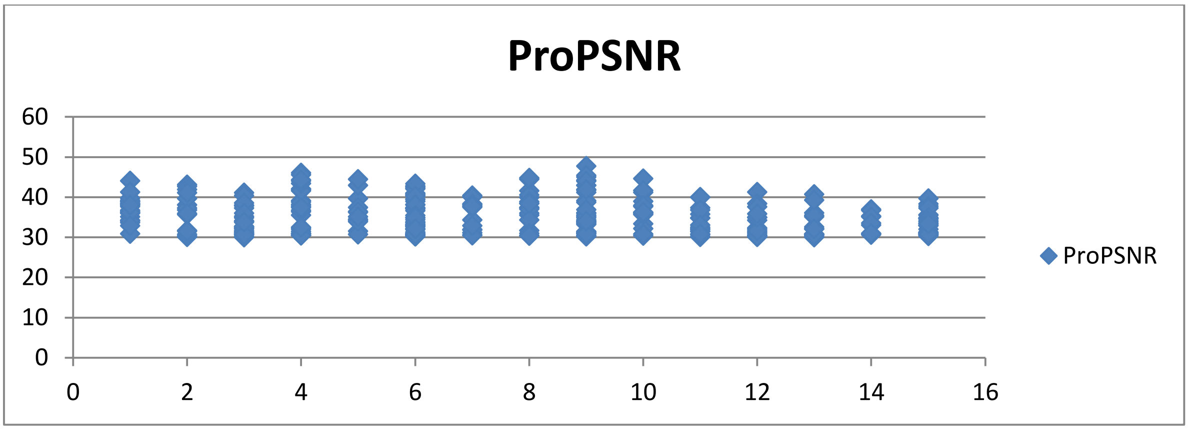


Figure 5.8: PSNR range for generated hiding patterns

5.4. Image quality Test for proposed method

5.4.1. Analysis of Normalized Cross Correlation

The image quality is another important requirement to investigate the performance of the JPEG steganography method and it is evaluated by assessing the similarity of cover and stego images in the system. The similarity between cover and stego images can be measured by using Normalized Cross Correlation function which is a statistical error measurement that used to measure the similarity between two digital images [84]. The Figure 5.9 shows NCC for both standard data hiding and proposed method with four modified quantization tables. If the NCC value is same, both cover and stego images in this system are identical to each other and it reveals that the NCC values for the proposed method in most cases are greater than the standard data hiding method. This shows that the proposed method that hides secrete message bits in lower frequencies provides better results in terms of image quality.

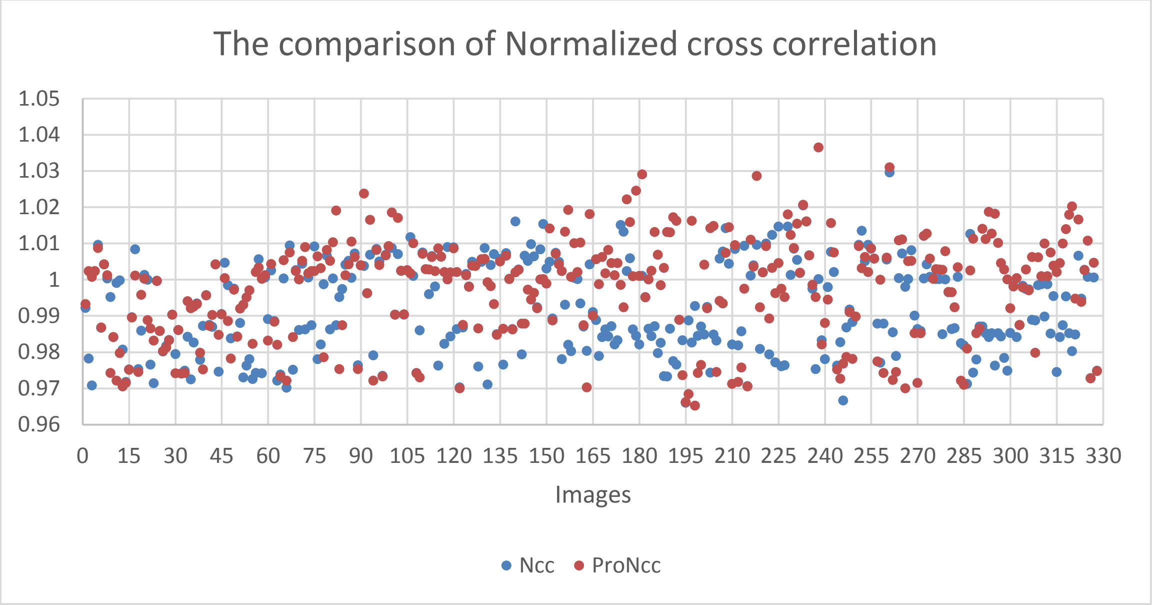


Figure 5.9: The Comparison of NCC for standard hiding method and proposed hiding method.

5.4.2. Analysis of Structural Content

Another image quality parameter, called structural content, is analyzed to evaluate the performance of the proposed system. Figure 5.10 illustrates the comparison between the proposed method and standard data hiding method in terms of image quality. This obliviously reveals that the quality of stego images in the proposed method is better than the standard data hiding method.

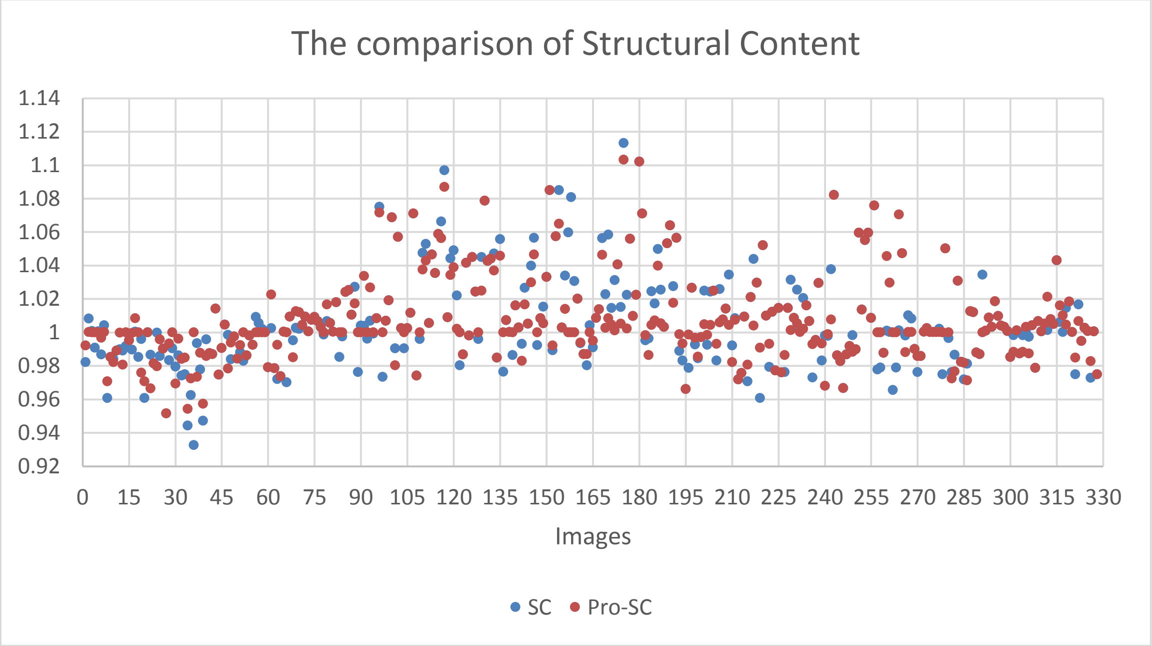


Figure 5.10: The comparison of SC values for standard hiding method and proposed hiding method.

5.4.3. Analysis of Relative Entropy (RE)

Relative entropy is derived based on the probability distribution of cover and stego image in the Equation and it is zero indicates that the image steganography system is perfect secure [54]. The figure 5.11 below indicates that the relative entropy of the most of the images goes to zero and nearly equal to zero. Finally, we argue that the stego image is secure based on the quality parameter.

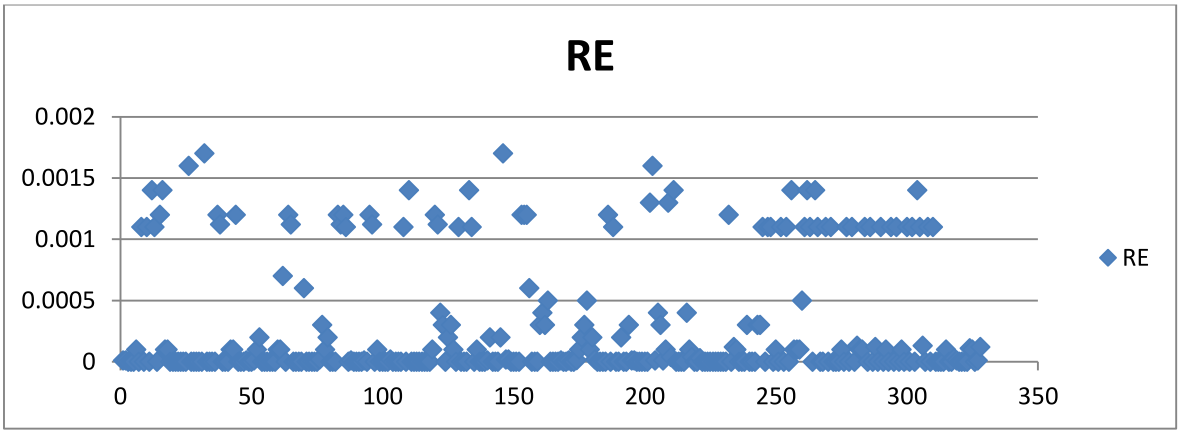


Figure 5.11: The results of relative entropy of cover and stego image set.

5.5. Embedding capacity of proposed randomly generated hiding patterns in lower frequencies

AS in the chapter 4, the randomly generated data hiding patterns contain the standard data hiding pattern in the literature and additional data hiding locations and number of bits used to hide in the DCT coefficients. According to them, the middle frequencies elements are replaced with two least significant of secrete message bits and lower frequency elements are only replaced with one least significant bit of secrete message bits. The embedding capacity of each pattern is displayed below in the table. The middle frequency data hiding uses 26 × 2 = 52 bits per block. The total image hides 52 × 1024 = 53248 bits size of secrete message. This technique is coded with MATLAB for our image dataset and the good indication of extracted PSNR values is the motivation for the proposed work that jumps to hide data in lower frequencies. The every generated patterns hide more secrete message bits than 53248 bits as we use the middle frequency data hiding included in every patterns.

Table 5.5: Data hiding patterns with maximum message size

Patterns (location, size)	Capacity (bits)	Bits/block
P1	55296	54
P2	56320	55
P3	57344	56
P4	56320	55
P5	56320	55
P6	55296	54
P7	56320	55
P8	56320	55
P9	55296	54
P10	56320	55

P11	58368	57
P12	58368	57
P13	58368	57
P14	58368	57
P15	58368	57

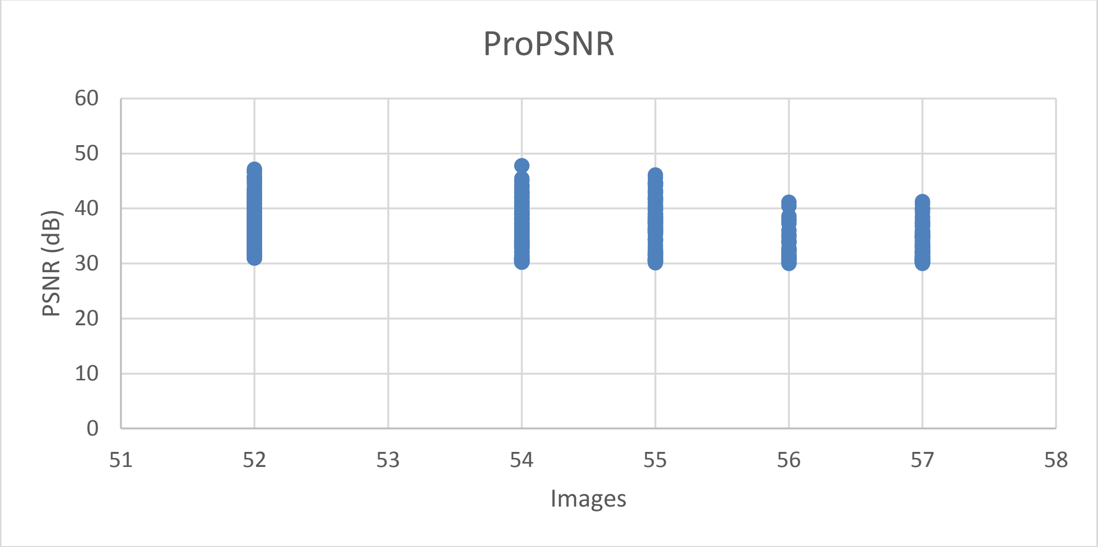


Figure 5.12: Comparison of PSNR range for standard hiding and proposed method

The standard hiding method hides two bits in middle frequency area for an image set. It hides 52 bits per block. In the proposed method, additionally, the lower frequency area also is utilized with middle frequency area to embed secret message bits. It is obviously state that the number of bits per block for image set is increased in the proposed method. Some locations of lower frequency area are used to hide one bit. Finally, the embedding capacities per block for the image set are 54, 55, 56 and 57. Figure 5.12 shows the PSNR range for the bits per block (52bits) in the standard hiding pattern and the PSNR range for the bits per block (54, 55, 56, and 57 bits) in the proposed method. The significance of the proposed PSNR and standard hiding method has been discussed in the Figure 5.5.

5.6. The results of file size

The stego file size is compared with the cover file size in terms of data embedding effect. Data hiding techniques in higher frequencies always increase the stego file size in terms of compression while lower frequency and data hiding techniques yield rational stego file size [58]. Here, it has been investigated the stego file size of the stego dataset with the cover image dataset. It shows the competitive results displayed in Figure 5.12 in terms of data embedding techniques used in proposed method.

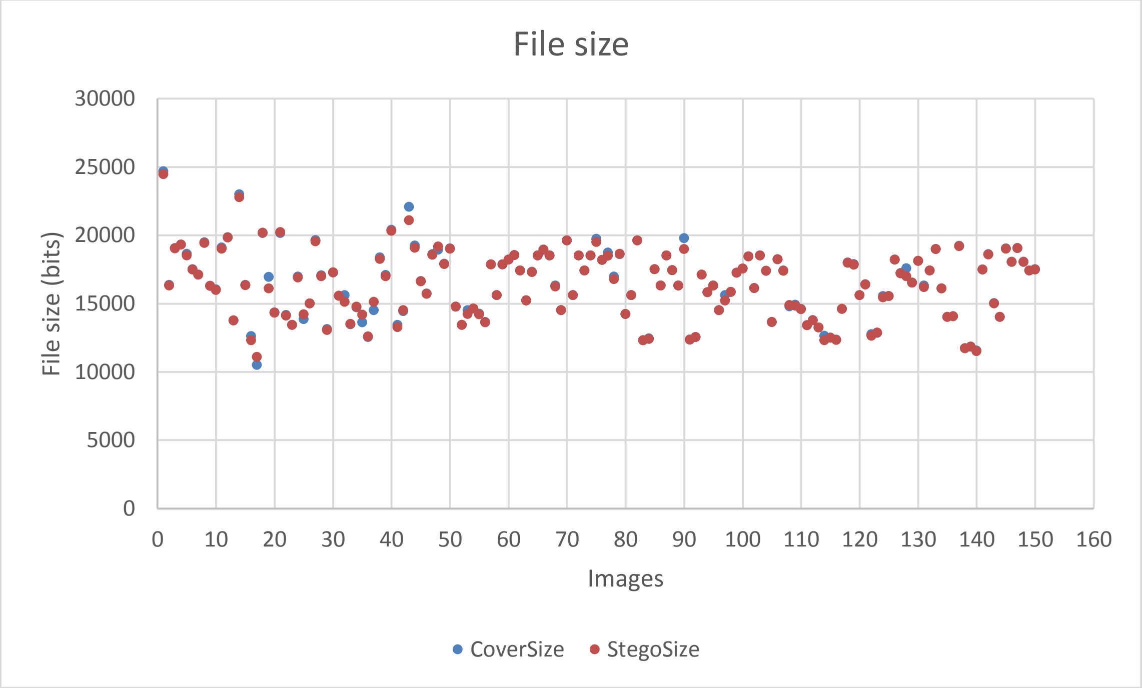


Figure 5.13: The analysis of cover and stego image file size

5.7. Relationship between the quantization table, data hiding patterns and image features – Identification Model

The selected features extracted from cover images are mapped with derive quantization table and data hiding pattern for an image using R and finally, the identification model is derived to identify the appropriate quantization table and data hiding pattern for an image based on image feature. So many investigations were carried out in this experimental study. However, based on the P-Value, we can conclude the relationship between the parameters. The results of the investigation are as follows:

5.7.1. Identification Model

Results 1: Combining the statistical features of DCT coefficients (DCT mean and DCT std) of cover images with Quantization Table (QT) using R library

```
> a=lm(QT~X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11 + X12 +
X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20,data=data)

> Summary (a)

Residual standard error: 0.8797 on 635 degrees of freedom

Multiple R-squared:  0.06919,   Adjusted R-squared:  0.03988

F-statistic:  2.36 on 20 and 635 DF, p-value: 0.0007634 – Positive Relationship
```

<u>Model</u>

```
Coefficients:
(Intercept)        X1            X2            X3          X4           X5
 2.006e+00   5.143e-04  -3.603e-03    6.261e-03   -1.215e-02    4.043e-02
     X6           X7          X8           X9        X10          X11
 1.230e-02  -1.344e-02  -2.043e-02  -3.821e-02   -1.638e-02   -9.969e-06
     X12          X13         X14          X15       X16          X17
 9.342e-03  -1.342e-02   3.172e-02  -1.633e-02    -9.335e-03   -5.408e-03
     X18          X19          X20
 3.509e-02    -1.074e-02   -1.851e-02
```

Results 2: Combining the statistical features of DCT elements (DCT-mean, DCT-std) of cover images with data hiding Pattern

```
> a=lm(Patt~X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11 + X12 +
X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20,data=data)

> Summary (a)

Residual standard error: 3.982 on 635 degrees of freedom

Multiple R-squared:  0.1471,    Adjusted R-squared:  0.1202

F-statistic: 5.476 on 20 and 635 DF, p-value: 4.598e-13  < 0.05 Positive relationship
```

Model

```
Coefficients:
(Intercept)        X1           X2          X3           X4         X5
  5.8800266   -0.0005198   0.0373551   0.0065309   -0.0095197  0.0805030
     X6            X7           X8          X9          X10        X11
-0.0845951     0.2108195   -0.4473427  -0.2342216  0.0263684   0.0020615
     X12           X13          X14         X15         X16        X17
  0.0523471    0.0172489   0.0136415  -0.1382812  -0.1356348   0.1124124
     X18           X19          X20
0.1355000      0.0296486   -0.0551435
```

5.8. Model validation

The statistical identification models that incorporates mean and standard deviation of lower frequency DCT element distribution is fitted to identify the modified quantization table and relevant data hiding pattern for selected image set. The model is used by the sender to find the modified quantization table and data hiding pattern and the same model is used by receiver to extract the secrete message. The proposed model based steganography scenario does not allow share secrete key between sender and receiver. The relevant generated stego images were tested in this research study to satisfy the statistical model. The experimental results show the 100% accuracy for image set. The results of the model validation is detailed in the Table 5.6 that shows the results of practical module, results of cover images whose features fitted to identification model and the results of stego images whose features fitted to the same model. The QT (Quantization Table) and Patt (Hiding Patterns) are detailed in every module.

Table 5.6: Results of the model validation for MIT Forest Images

				Cover Image-set		Stego-Imageset	
image	QT	Patt	PSNR	Model-QT	Model-Patt	Model-QT	Model-Patt
image_0001	2	11	34.7913	2.12E+00	1.11E+01	2.20E+00	1.15E+01
image_0002	1	15	32.9673	9.60E-01	1.51E+01	1.11E+00	1.52E+01
image_0003	2	6	42.7909	1.96E+00	6.32E+00	1.92E+00	6.36E+00
image_0004	1	11	37.3219	1.02E+00	1.12E+01	9.50E-01	1.13E+01
image_0005	4	13	35.1275	3.82E+00	1.35E+01	3.96E+00	1.35E+01
image_0006	3	10	41.1919	3.31E+00	1.02E+01	3.01E+00	1.04E+01
image_0007	2	9	44.9914	2.10E+00	9.36E+00	2.23E+00	9.39E+00
image_0008	2	2	43.1303	2.01E+00	2.34E+00	2.35E+00	2.46E+00
image_0009	2	4	38.1902	2.10E+00	4.12E+00	2.31E+00	4.36E+00
image_0010	2	9	44.2559	2.21E+00	9.02E+00	1.98E+00	9.36E+00
image_0011	1	8	35.5054	1.06E+00	8.42E+00	8.92E-01	8.50E+00
image_0012	3	4	37.7512	3.24E+00	4.44E+00	3.00E+00	4.50E+00
image_0013	3	10	38.974	3.26E+00	1.05E+01	3.24E+00	1.03E+01
image_0014	3	12	31.3296	2.96E+00	1.20E+01	3.34E+00	1.24E+01
image_0015	2	2	36.812	2.19E+00	2.22E+00	2.36E+00	2.41E+00
image_0016	2	7	34.3084	2.36E+00	7.35E+00	2.50E+00	7.38E+00
image_0017	2	6	37.3869	2.02E+00	5.96E+00	2.01E+00	6.34E+00
image_0018	2	6	42.2786	2.50E+00	6.28E+00	2.36E+00	6.42E+00
image_0019	2	11	35.8024	1.81E+00	1.09E+01	2.14E+00	1.10E+01
image_0020	2	8	39.9171	2.36E+00	8.00E+00	2.04E+00	8.23E+00
image_0021	2	9	47.7553	2.36E+00	9.24E+00	2.22E+00	9.24E+00
image_0022	3	6	37.3169	2.89E+00	6.38E+00	3.26E+00	6.37E+00
image_0023	2	8	37.3712	2.31E+00	8.29E+00	2.36E+00	8.42E+00
image_0024	2	4	39.0788	1.85E+00	4.44E+00	2.14E+00	4.36E+00
image_0025	2	7	27.8157	2.15E+00	7.12E+00	2.34E+00	7.25E+00
image_0026	2	9	36.0583	2.01E+00	9.41E+00	1.90E+00	9.43E+00
image_0027	2	13	32.5734	2.00E+00	1.32E+01	2.46E+00	1.33E+01
image_0028	4	7	31.1591	4.36E+00	7.01E+00	4.50E+00	7.13E+00
image_0029	3	8	41.581	3.33E+00	8.47E+00	3.00E+00	8.26E+00
image_0030	3	15	38.3341	3.31E+00	1.52E+01	3.24E+00	1.54E+01
image_0031	3	13	36.1075	3.12E+00	1.31E+01	3.23E+00	1.31E+01
image_0032	2	11	24.9183	1.94E+00	1.15E+01	2.37E+00	1.12E+01
image_0033	3	1	39.1964	3.23E+00	1.09E+00	3.21E+00	1.02E+00
image_0034	3	8	36.0367	2.87E+00	8.11E+00	3.23E+00	8.35E+00
image_0035	2	7	37.5269	2.15E+00	7.21E+00	2.14E+00	7.41E+00
image_0036	2	2	38.0938	2.16E+00	2.12E+00	2.42E+00	2.02E+00
image_0037	1	3	20.6348	1.33E+00	3.24E+00	1.04E+00	3.02E+00
image_0038	2	9	26.4747	2.10E+00	9.00E+00	1.99E+00	9.40E+00

image_0039	3	8	37.4128	3.00E+00	8.23E+00	3.24E+00	8.09E+00
image_0040	2	12	41.2437	1.86E+00	1.21E+01	2.01E+00	1.21E+01
image_0041	2	3	41.132	2.52E+00	3.23E+00	2.34E+00	3.12E+00
image_0042	2	12	30.5469	2.41E+00	1.21E+01	2.12E+00	1.20E+01
image_0043	2	8	40.5322	1.71E+00	8.34E+00	2.00E+00	8.40E+00
image_0044	3	13	35.4222	2.91E+00	1.32E+01	3.46E+00	1.32E+01
image_0045	4	4	42.0545	4.50E+00	4.23E+00	4.24E+00	4.24E+00
image_0046	2	6	42.6658	2.33E+00	6.46E+00	2.34E+00	6.32E+00
image_0047	3	8	44.4845	3.23E+00	7.79E+00	3.24E+00	8.42E+00
image_0048	4	1	38.1399	4.01E+00	1.26E+00	4.46E+00	1.02E+00
image_0049	2	1	44.0316	2.22E+00	1.43E+00	2.14E+00	1.12E+00
image_0050	2	4	41.9053	2.12E+00	4.00E+00	2.33E+00	4.12E+00
image_0051	3	3	38.0329	3.01E+00	3.13E+00	3.46E+00	3.66E+00
image_0052	2	15	39.6747	2.01E+00	1.53E+01	2.12E+00	1.54E+01
image_0053	1	4	36.4264	1.45E+00	4.00E+00	1.49E+00	4.45E+00
image_0054	2	3	40.4238	2.01E+00	3.00E+00	2.14E+00	3.67E+00
image_0055	4	11	34.8204	4.12E+00	1.12E+01	4.49E+00	1.13E+01
image_0056	4	2	42.6864	4.91E+00	1.90E+00	4.50E+00	2.13E+00
image_0057	3	3	34.9169	3.33E+00	3.34E+00	3.34E+00	3.34E+00
image_0058	3	10	44.6667	3.00E+00	1.03E+01	3.33E+00	1.03E+01
image_0059	2	9	45.4366	2.01E+00	9.01E+00	2.22E+00	9.12E+00
image_0060	2	4	38.7845	1.59E+00	4.10E+00	2.24E+00	4.23E+00
image_0061	2	3	35.1913	2.35E+00	3.12E+00	2.51E+00	3.52E+00
image_0062	3	5	39.6626	2.65E+00	5.45E+00	3.12E+00	5.52E+00
image_0063	4	8	37.0232	4.50E+00	8.01E+00	4.24E+00	8.62E+00
image_0064	3	6	37.1036	2.91E+00	6.19E+00	3.21E+00	6.32E+00
image_0065	2	11	40.0116	2.01E+00	1.10E+01	2.14E+00	1.14E+01
image_0066	2	1	38.3958	1.87E+00	1.12E+00	2.34E+00	1.01E+00
image_0067	3	6	40.5201	3.31E+00	6.13E+00	3.24E+00	6.26E+00
image_0068	3	1	38.8847	3.33E+00	1.42E+00	3.36E+00	1.03E+00
image_0069	2	6	40.9888	1.65E+00	6.00E+00	2.36E+00	6.35E+00
image_0070	3	9	42.9521	3.12E+00	9.50E+00	3.33E+00	9.12E+00
image_0071	3	6	37.1036	2.96E+00	5.85E+00	3.00E+00	6.32E+00
image_0072	2	11	40.0116	2.31E+00	1.14E+01	2.35E+00	1.15E+01
image_0073	2	1	38.3958	2.15E+00	1.07E+00	2.23E+00	1.13E+00
image_0074	3	6	40.5201	3.45E+00	6.00E+00	3.24E+00	6.42E+00
image_0075	2	15	35.6043	2.16E+00	1.54E+01	2.32E+00	1.55E+01
image_0076	2	6	39.4104	2.14E+00	6.32E+00	2.23E+00	6.35E+00
image_0077	3	1	38.8847	3.24E+00	1.50E+00	3.33E+00	1.23E+00
image_0078	2	6	40.9888	1.91E+00	6.12E+00	2.00E+00	6.42E+00
image_0079	3	9	42.9521	3.46E+00	9.33E+00	3.49E+00	9.32E+00
image_0080	2	9	41.7485	1.90E+00	9.12E+00	2.01E+00	9.37E+00

image_0081	3	3	37.8163	2.91E+00	3.45E+00	3.41E+00	3.45E+00
image_0082	2	5	36.2696	2.46E+00	5.46E+00	2.30E+00	5.47E+00
image_0083	3	6	34.3798	3.01E+00	5.90E+00	3.50E+00	6.42E+00
image_0084	2	2	37.2978	1.95E+00	2.42E+00	2.04E+00	2.25E+00
image_0085	2	13	40.7525	2.35E+00	1.35E+01	2.38E+00	1.35E+01
image_0086	2	12	35.0048	2.14E+00	1.23E+01	2.22E+00	1.20E+01
image_0087	2	8	38.8784	2.30E+00	8.45E+00	2.37E+00	8.23E+00
image_0088	2	5	37.4126	2.00E+00	5.46E+00	2.42E+00	5.24E+00
image_0089	4	10	36.1442	3.81E+00	1.04E+01	4.48E+00	1.00E+01
image_0090	3	9	33.9032	3.23E+00	8.56E+00	3.34E+00	9.00E+00
image_0091	3	9	33.9032	3.34E+00	9.10E+00	3.41E+00	9.25E+00
image_0092	2	10	41.6989	1.89E+00	1.03E+01	2.00E+00	1.00E+01
image_0093	2	13	39.2799	2.01E+00	1.34E+01	2.00E+00	1.31E+01
image_0094	2	14	35.2605	1.78E+00	1.40E+01	2.37E+00	1.42E+01
image_0095	2	4	46.0866	2.13E+00	4.26E+00	2.19E+00	4.05E+00
image_0096	1	10	33.3639	1.23E+00	1.05E+01	1.36E+00	1.02E+01
image_0097	4	4	41.6077	4.25E+00	4.41E+00	4.45E+00	4.46E+00
image_0098	1	13	26.2692	1.11E+00	1.30E+01	1.25E+00	1.36E+01
image_0099	1	6	32.1887	1.25E+00	6.42E+00	1.38E+00	6.36E+00
image_0100	4	15	23.8879	4.23E+00	1.50E+01	4.38E+00	1.52E+01
image_0101	4	6	42.0917	4.13E+00	6.01E+00	4.37E+00	6.09E+00
image_0102	3	9	34.9163	3.22E+00	9.01E+00	3.24E+00	9.08E+00
image_0103	2	4	43.3962	2.01E+00	4.52E+00	2.41E+00	4.53E+00
image_0104	2	7	40.3669	2.22E+00	7.40E+00	2.36E+00	7.48E+00
image_0105	4	2	41.9106	4.33E+00	2.22E+00	4.55E+00	1.78E+00
image_0106	3	2	35.6476	3.34E+00	2.44E+00	3.50E+00	2.09E+00
image_0107	3	6	29.5739	3.21E+00	6.23E+00	3.36E+00	6.25E+00
image_0108	4	15	37.782	4.12E+00	1.53E+01	4.29E+00	1.52E+01
image_0109	3	1	34.2233	3.47E+00	1.49E+00	3.33E+00	1.38E+00
image_0110	3	6	29.6472	3.25E+00	5.68E+00	3.34E+00	6.01E+00
image_0111	3	13	30.8494	3.27E+00	1.33E+01	3.46E+00	9.16E-01
image_0112	1	9	30.5171	1.37E+00	9.12E+00	9.99E-01	9.38E+00
image_0113	1	9	31.1031	7.86E-01	9.23E+00	1.10E+00	9.08E+00
image_0114	2	15	33.3587	2.01E+00	1.52E+01	2.22E+00	1.54E+01
image_0115	2	3	30.5367	2.16E+00	3.37E+00	2.36E+00	3.33E+00
image_0116	4	6	29.8922	4.00E+00	6.12E+00	4.11E+00	6.01E+00
image_0117	1	10	28.4079	1.20E+00	1.04E+01	1.32E+00	1.20E+00
image_0118	1	8	31.6879	7.65E-01	8.27E+00	1.50E+00	8.45E+00
image_0119	4	5	31.5024	4.26E+00	5.42E+00	4.41E+00	5.41E+00
image_0120	2	11	32.5228	2.01E+00	1.13E+01	2.36E+00	1.15E+01
image_0121	4	7	38.0459	4.33E+00	7.47E+00	4.39E+00	7.48E+00
image_0122	1	6	36.6522	8.95E-01	6.46E+00	1.39E+00	6.01E+00

image_0123	4	9	31.3893	3.78E+00	8.70E+00	3.99E+00	9.08E+00
image_0124	2	3	32.2819	2.01E+00	3.43E+00	2.00E+00	3.49E+00
image_0125	2	9	44.0143	2.30E+00	9.00E+00	2.04E+00	9.08E+00
image_0126	3	12	38.4363	3.01E+00	1.20E+01	3.24E+00	1.40E+00
image_0127	3	9	33.6619	3.00E+00	9.33E+00	3.01E+00	9.17E+00
image_0128	2	3	29.1793	2.12E+00	3.45E+00	2.37E+00	3.50E+00
image_0129	3	6	33.2135	3.33E+00	6.05E+00	3.45E+00	6.01E+00
image_0130	2	10	32.2016	1.65E+00	1.00E+01	2.22E+00	1.04E+01
image_0131	1	9	30.9765	1.50E+00	9.34E+00	1.38E+00	9.38E+02
image_0132	2	3	37.2862	1.87E+00	3.33E+00	2.22E+00	3.24E+00
image_0133	4	10	36.1634	4.00E+00	1.01E+01	4.18E+00	1.04E+01
image_0134	2	4	35.5131	2.13E+00	4.17E+00	2.37E+00	4.49E+00
image_0135	3	1	35.1283	3.21E+00	1.01E+00	3.24E+00	1.02E+00
image_0136	4	4	31.4457	3.67E+00	4.19E+00	4.15E+00	4.44E+00
image_0137	4	15	30.4628	3.88E+00	1.50E+01	4.12E+00	1.50E+01
image_0138	3	12	30.1976	3.01E+00	1.23E+01	3.46E+01	1.45E+00
image_0139	1	6	33.6179	1.30E+00	6.33E+00	1.38E+00	6.01E+00
image_0140	2	15	34.7108	2.30E+00	1.52E+01	2.12E+00	1.54E+01
image_0141	1	3	31.1516	1.01E+00	3.50E+00	1.10E+00	3.46E+00
image_0142	1	7	29.5772	1.36E+00	7.33E+00	1.39E+00	7.29E+00
image_0143	3	9	34.3506	3.21E+00	9.12E+00	3.43E+00	9.17E+00
image_0144	3	3	32.4615	3.00E+00	3.41E+00	3.69E+00	3.41E+00
image_0145	4	15	31.0328	4.00E+00	1.50E+01	4.24E+00	1.54E+01
image_0146	2	15	29.7061	2.01E+00	1.49E+01	2.14E+00	1.50E+01
image_0147	3	12	37.5662	3.24E+00	1.22E+01	3.29E+00	1.21E+01
image_0148	2	12	30.3286	2.01E+00	1.24E+01	2.37E+00	1.25E+01
image_0149	1	9	27.2311	1.24E+00	8.79E+00	1.35E+00	9.17E+00
image_0150	2	1	33.7065	1.98E+00	1.36E+00	2.42E+00	1.00E+00
image_0151	3	11	31.5319	3.45E+00	1.09E+01	3.46E+00	1.10E+01
image_0152	3	6	33.1656	3.27E+00	6.46E+00	3.50E+00	6.01E+00
image_0153	4	15	30.6894	4.19E+00	1.52E+01	4.38E+00	1.53E+01
image_0154	2	15	34.7108	1.89E+00	1.55E+01	2.22E+00	1.53E+01
image_0155	2	15	34.7108	1.60E+00	1.55E+01	2.00E+00	1.50E+01
image_0156	2	6	33.0276	2.12E+00	6.12E+00	2.37E+00	6.32E+00
image_0157	2	13	32.0827	2.12E+00	1.32E+01	2.37E+00	1.30E+01
image_0158	4	15	35.5224	4.13E+00	1.48E+01	4.39E+00	1.52E+01
image_0159	2	2	39.7011	2.10E+00	2.12E+00	2.22E+00	2.23E+00
image_0160	2	14	36.9273	2.00E+00	1.43E+01	2.37E+00	1.43E+01
image_0161	2	7	40.1139	2.01E+00	7.25E+00	2.24E+00	7.19E+00
image_0162	1	5	36.4409	1.38E+00	5.46E+00	1.48E+00	5.21E+00
image_0163	2	1	34.1027	2.00E+00	1.28E+00	2.37E+00	1.11E+00
image_0164	2	10	37.6888	2.35E+00	1.00E+01	2.46E+00	1.01E+01

image_0165	2	6	43.3808	2.01E+00	6.39E+00	2.23E+00	6.01E+00
image_0166	2	4	45.5694	2.01E+00	4.29E+00	2.37E+00	4.14E+00
image_0167	4	15	29.3006	4.38E+00	1.52E+01	4.50E+00	1.54E+01
image_0168	2	6	30.6409	2.01E+00	6.45E+00	2.37E+00	6.79E+00
image_0169	3	11	31.4822	3.01E+00	1.15E+01	3.34E+00	1.15E+01
image_0170	3	6	32.7031	3.26E+00	5.89E+00	3.47E+00	6.24E+00
image_0171	4	15	31.0893	4.26E+00	1.54E+01	4.31E+00	1.55E+01
image_0172	2	9	35.5625	2.00E+00	9.33E+00	2.50E+00	9.17E+00
image_0173	3	13	28.84	3.34E+00	1.35E+01	3.47E+00	1.31E+01
image_0174	2	1	35.9749	1.75E+00	1.39E+00	2.37E+00	1.02E+00
image_0175	4	5	27.748	4.23E+00	5.42E+00	4.28E+00	5.47E+00
image_0176	4	1	37.7054	4.01E+00	1.12E+00	4.09E+00	1.49E+00
image_0177	3	15	32.9044	3.33E+00	1.54E+01	3.01E+00	1.53E+01
image_0178	3	13	30.6498	3.22E+00	1.30E+01	3.26E+00	1.34E+01
image_0179	2	15	31.156	2.50E+00	1.53E+01	2.37E+00	1.53E+01
image_0180	2	6	27.2427	2.00E+00	6.42E+00	2.37E+00	6.41E+00
image_0181	1	2	30.1078	1.44E+00	2.34E+00	1.50E+00	2.50E+00
image_0182	3	6	39.4803	3.45E+00	6.22E+00	3.33E+00	6.01E+00
image_0183	3	4	36.6913	3.23E+00	4.38E+00	3.46E+00	4.01E+00
image_0184	4	8	29.3761	3.63E+00	8.34E+00	4.24E+00	8.08E+00
image_0185	3	10	35.894	3.23E+00	9.90E+00	3.43E+00	1.04E+01
image_0186	2	3	34.0999	2.50E+00	3.40E+00	2.37E+00	3.33E+00
image_0187	3	6	34.8713	3.01E+00	6.48E+00	3.34E+00	6.41E+00
image_0188	3	12	32.3583	3.59E+00	1.24E+01	3.34E+00	1.22E+01
image_0189	2	6	33.8819	2.37E+00	6.50E+00	2.35E+00	6.45E+00
image_0190	3	4	31.9998	3.33E+00	4.19E+00	3.24E+00	4.43E+00
image_0191	2	8	34.349	2.42E+00	8.00E+00	2.45E+00	8.07E+00
image_0192	2	3	29.7896	2.36E+00	3.32E+00	2.38E+00	3.29E+00
image_0193	1	12	30.4038	1.24E+00	1.20E+01	1.36E+00	1.20E+01
image_0194	1	4	29.4904	1.00E+00	4.39E+00	1.31E+00	4.12E+00
image_0195	2	15	32.0278	1.79E+00	1.51E+01	2.37E+00	1.52E+01
image_0196	1	11	32.1776	1.24E+00	1.14E+01	1.26E+00	1.15E+01
image_0197	3	1	36.6873	3.33E+00	1.45E+00	3.46E+00	1.09E+00
image_0198	3	3	30.8549	3.45E+00	3.12E+00	3.50E+00	3.09E+00
image_0199	3	4	30.9414	3.12E+00	4.22E+00	3.24E+00	4.09E+00
image_0200	3	3	31.5175	3.23E+00	3.36E+00	3.20E+00	3.40E+00
image_0201	2	6	38.934	2.19E+00	6.33E+00	2.37E+00	6.39E+00
image_0202	3	12	29.3595	3.00E+00	1.24E+01	3.42E+00	1.24E+01
image_0203	2	15	31.2455	2.21E+00	1.52E+01	2.37E+00	1.50E+01
image_0204	3	15	31.2789	3.22E+00	1.50E+01	3.46E+00	1.53E+01
image_0205	3	4	27.9058	3.10E+00	4.13E+00	3.41E+00	4.02E+00
image_0206	4	5	34.4475	4.50E+00	5.42E+00	4.49E+00	5.50E+00

image_0207	4	4	37.4198	4.25E+00	4.00E+00	4.26E+00	4.34E+00
image_0208	1	11	28.6457	1.01E+00	1.14E+01	1.05E+00	1.12E+01
image_0209	4	13	29.0179	4.13E+00	1.34E+01	4.25E+00	1.32E+01
image_0210	3	12	30.1258	3.40E+00	1.24E+01	3.24E+00	1.21E+01
image_0211	2	3	38.5526	2.36E+00	3.33E+00	2.42E+00	3.40E+00
image_0212	2	3	32.6088	2.41E+00	3.33E+00	2.50E+00	3.48E+00
image_0213	3	2	29.3463	3.01E+00	2.50E+00	3.56E+00	2.23E+00
image_0214	2	9	39.0954	2.52E+00	9.37E+00	2.37E+00	9.17E+00
image_0215	3	5	34.2783	3.42E+00	5.40E+00	3.50E+00	5.12E+00
image_0216	3	13	32.0634	3.12E+00	1.32E+01	3.33E+00	1.34E+01
image_0217	3	6	32.9035	3.40E+00	6.42E+00	3.12E+00	6.02E+00
image_0218	3	2	31.6975	3.00E+00	2.00E+00	3.45E+00	2.20E+00
image_0219	3	12	32.0029	3.25E+00	1.20E+01	3.50E+00	1.20E+01
image_0220	4	11	36.7875	3.78E+00	1.12E+01	4.50E+00	1.13E+01
image_0221	3	3	31.2405	3.46E+00	3.21E+00	3.50E+00	3.49E+00
image_0222	2	6	40.2474	2.37E+00	6.33E+00	2.36E+00	6.48E+00
image_0223	1	1	26.912	9.00E-01	1.38E+00	1.07E+00	1.22E+00
image_0224	4	7	31.9473	4.26E+00	7.50E+00	4.29E+00	7.36E+00
image_0225	1	12	30.96	1.50E+00	1.20E+01	1.46E+00	1.17E+01
image_0226	3	9	41.1673	2.79E+00	9.12E+00	3.34E+00	9.37E+00
image_0227	3	3	29.0004	3.33E+00	3.48E+00	3.26E+00	3.50E+00
image_0228	3	6	32.6789	3.12E+00	6.00E+00	3.34E+00	6.04E+00
image_0229	1	6	29.9863	1.01E+00	6.00E+00	1.36E+00	6.43E+00
image_0230	2	9	38.7534	2.45E+00	9.00E+00	2.15E+00	9.37E+00
image_0231	2	2	35.9113	1.66E+00	2.37E+00	2.18E+00	2.23E+00
image_0232	4	13	29.6385	4.39E+00	1.33E+01	4.41E+00	1.31E+01
image_0233	3	1	39.7699	3.12E+00	1.29E+00	3.24E+00	1.09E+00
image_0234	2	15	37.2668	1.90E+00	1.49E+01	2.49E+00	1.54E+01
image_0235	2	10	36.1356	2.13E+00	1.05E+01	2.37E+00	1.00E+01
image_0236	1	11	29.1655	1.01E+00	1.10E+01	1.06E+00	1.13E+01
image_0237	4	7	38.3495	4.17E+00	7.49E+00	4.28E+00	7.10E+00
image_0238	3	14	36.6909	2.79E+00	1.42E+01	3.44E+00	1.41E+01
image_0239	4	15	33.8271	4.28E+00	1.52E+01	4.39E+00	1.54E+01
image_0240	1	6	31.3011	1.02E+00	6.26E+00	1.24E+00	6.27E+00
image_0241	3	15	34.5835	3.00E+00	1.55E+01	3.50E+00	1.52E+01
image_0242	2	3	32.1102	2.31E+00	3.48E+00	2.45E+00	3.42E+00
image_0243	3	6	28.4578	2.91E+00	6.33E+00	3.45E+00	6.12E+00
image_0244	3	2	29.7274	3.00E+00	2.13E+00	3.45E+00	2.43E+00
image_0245	4	15	29.8036	3.81E+00	1.53E+01	4.23E+00	1.54E+01
image_0246	3	8	29.9625	2.86E+00	8.50E+00	3.34E+00	8.39E+00
image_0247	1	6	30.5579	1.23E+00	6.45E+00	1.50E+00	6.18E+00
image_0248	3	9	33.2009	3.33E+00	9.50E+00	3.24E+00	9.37E+00

image_0249	4	6	38.1519	3.67E+00	6.41E+00	4.25E+00	6.05E+00
image_0250	1	4	29.5122	1.46E+00	4.39E+00	1.49E+00	4.40E+00
image_0251	2	14	35.0895	2.10E+00	1.42E+01	2.36E+00	1.41E+01
image_0252	2	4	44.0858	2.30E+00	4.20E+00	2.32E+00	4.37E+00
image_0253	2	10	35.6806	2.21E+00	1.02E+01	2.36E+00	1.01E+01
image_0254	3	15	33.4856	2.71E+00	1.52E+01	3.23E+00	1.54E+01
image_0255	1	3	32.7196	1.01E+00	3.46E+00	1.09E+00	3.45E+00
image_0256	2	12	34.2177	1.58E+00	1.24E+01	2.37E+00	1.25E+01
image_0257	1	13	28.5722	8.10E-01	1.30E+01	1.03E+00	1.32E+01
image_0258	1	6	28.8292	7.30E-01	6.47E+00	1.08E+00	6.41E+00
image_0259	2	6	30.2842	1.99E+00	6.23E+00	2.16E+00	6.39E+00
image_0260	4	12	29.2566	4.50E+00	1.22E+01	4.50E+00	1.23E+01
image_0261	2	1	36.4198	2.12E+00	1.39E+00	2.19E+00	1.10E+00
image_0262	2	6	38.045	2.13E+00	6.12E+00	2.42E+00	6.45E+00
image_0263	3	5	33.9653	3.01E+00	5.49E+00	3.44E+00	5.36E+00
image_0264	4	12	27.201	4.24E+00	1.20E+01	4.29E+00	1.21E+01
image_0265	2	14	33.0599	2.22E+00	1.43E+01	2.36E+00	1.45E+01
image_0266	4	10	37.9504	4.36E+00	1.02E+01	4.38E+00	1.01E+01
image_0267	3	14	29.6905	3.33E+00	1.43E+01	3.44E+00	1.41E+01
image_0268	2	13	30.7533	2.52E+00	1.33E+01	2.36E+00	1.35E+01
image_0269	1	10	26.8107	1.01E+00	1.00E+01	1.11E+00	1.00E+01
image_0270	2	5	42.9428	2.48E+00	5.19E+00	2.50E+00	1.16E+01
image_0271	3	11	29.1104	3.11E+00	1.14E+01	3.24E+00	1.13E+01
image_0272	2	3	26.1048	2.52E+00	3.47E+00	2.46E+00	3.23E+00
image_0273	3	4	32.3038	3.11E+00	4.14E+00	3.34E+00	4.36E+00
image_0274	3	15	34.9016	3.34E+00	1.54E+01	3.14E+00	1.55E+01
image_0275	3	3	33.9452	3.23E+00	3.34E+00	3.11E+00	2.89E+02
image_0276	4	9	33.4342	4.10E+00	9.12E+00	4.24E+00	9.37E+00
image_0277	3	1	36.1704	3.50E+00	1.49E+00	3.01E+00	6.80E-01
image_0278	3	8	29.4271	3.49E+00	8.19E+00	3.01E+00	8.07E+00
image_0279	2	13	29.5641	2.36E+00	1.32E+01	2.35E+00	1.35E+01
image_0280	4	14	23.9053	4.50E+00	1.43E+01	4.44E+00	1.44E+01
image_0281	4	13	32.0625	3.66E+00	1.30E+01	4.46E+00	1.32E+01
image_0282	1	6	31.9429	1.36E+00	5.89E+00	1.46E+00	6.25E+00
image_0283	2	4	29.891	2.10E+00	4.29E+00	2.34E+00	4.34E+00
image_0284	1	6	29.2644	1.37E+00	5.56E+00	1.49E+00	6.47E+00
image_0285	2	11	33.0857	1.85E+00	1.15E+01	2.12E+00	1.12E+01
image_0286	1	6	25.7046	1.24E+00	6.00E+00	1.38E+00	6.50E+00
image_0287	4	3	35.9704	3.79E+00	3.42E+00	4.12E+00	3.08E+00
image_0288	2	14	33.4945	1.87E+00	1.45E+01	2.10E+00	1.43E+01
image_0289	3	4	27.4882	2.57E+00	3.85E+00	3.24E+00	4.19E+00
image_0290	3	9	35.975	2.79E+00	8.75E+00	3.46E+00	9.37E+00

image_0291	3	1	32.8551	3.01E+00	1.12E+00	3.44E+00	1.09E+00
image_0292	2	5	44.4558	2.21E+00	5.11E+00	2.41E+00	5.08E+00
image_0293	2	11	29.8321	2.32E+00	1.10E+01	2.46E+00	1.10E+01
image_0294	3	9	28.9745	2.79E+00	9.45E+00	2.91E+00	9.37E+00
image_0295	4	12	31.6504	4.24E+00	1.19E+01	4.28E+00	1.25E+01
image_0296	4	3	27.6789	4.24E+00	3.00E+00	4.47E+00	3.45E+00
image_0297	2	4	44.2781	2.51E+00	4.13E+00	2.50E+00	4.11E+00
image_0298	2	10	36.2119	2.48E+00	9.86E+00	2.50E+00	1.01E+01
image_0299	1	9	27.25	9.12E-01	9.13E+00	1.12E+00	9.17E+00
image_0300	3	6	28.7094	3.23E+00	6.44E+00	3.44E+00	6.50E+00
image_0301	3	9	41.8756	3.00E+00	9.45E+00	3.45E+00	9.07E+00
image_0302	2	15	32.9539	1.85E+00	1.54E+01	2.46E+00	1.55E+01
image_0303	3	8	38.471	3.06E+00	8.01E+00	3.01E+00	8.07E+00
image_0304	1	2	31.5139	1.01E+00	2.22E+00	1.09E+00	2.33E+00
image_0305	2	15	34.0557	2.31E+00	1.54E+01	2.49E+00	1.54E+01
image_0306	2	7	25.5317	2.47E+00	7.06E+00	2.22E+00	7.31E+00
image_0307	3	8	44.7534	3.11E+00	8.04E+00	3.34E+00	8.07E+00
image_0308	2	5	35.1176	2.50E+00	5.12E+00	2.46E+00	5.34E+00
image_0309	4	9	30.9161	4.12E+00	9.13E+00	4.25E+00	9.37E+00
image_0310	2	9	35.2232	1.98E+00	9.49E+00	2.46E+00	9.37E+00
image_0311	3	12	34.9605	3.07E+00	1.18E+01	3.24E+00	1.23E+01
image_0312	3	1	41.2461	3.50E+00	1.37E+00	3.33E+00	1.45E+00
image_0313	3	12	35.8193	3.01E+00	1.20E+01	3.50E+00	1.25E+01
image_0314	2	3	33.7994	1.94E+00	3.37E+00	2.37E+00	3.32E+00
image_0315	2	15	30.6984	2.18E+00	1.55E+01	2.37E+00	1.53E+01
image_0316	2	6	35.4396	2.46E+00	6.33E+00	2.23E+00	6.41E+00
image_0317	3	6	34.9035	3.33E+00	6.44E+00	3.23E+00	6.23E+00
image_0318	3	2	41.0844	3.33E+00	2.12E+00	3.12E+00	2.22E+00
image_0319	2	1	37.9857	2.14E+00	1.00E+00	2.46E+00	1.09E+00
image_0320	3	7	37.7816	3.31E+00	7.12E+00	3.00E+00	7.48E+00
image_0321	4	8	38.4128	4.00E+00	8.37E+00	4.28E+00	8.09E+00
image_0322	2	9	36.8982	2.32E+00	9.33E+00	2.50E+00	9.37E+00
image_0323	3	15	33.3687	3.22E+00	1.46E+01	3.24E+00	1.52E+01
image_0324	3	4	32.5106	3.43E+00	4.26E+00	3.12E+00	4.23E+00
image_0325	4	6	32.1111	3.89E+00	6.41E+00	4.39E+00	6.50E+00
image_0326	4	14	29.9961	3.87E+00	1.42E+01	4.37E+00	1.45E+01
image_0327	2	7	32.9192	2.01E+00	7.41E+00	2.37E+00	7.23E+00
image_0328	2	9	33.9824	2.01E+00	9.00E+00	2.23E+00	9.12E+00

From the results extracted from the model, the extracted statistical features of cover and stego images are fitted into the model and the values of quantization table (QT) and data hiding pattern (Patt) are displayed in the Model-QT and Model-Patt columns under the Cover Image set and Stego Image set. To show the significance of extracted QT and Patt in both sender and receiver side, the accuracy is calculated. The MIT image set shows the good accuracy level. The analysis of F-Test Two-Sample for Variances is depicted for QT and Patt in the Tables 5.7 and 5.8.

Table 5.7: F-Test for QT

F-Test Two-Sample for Variances		
	Model-QT(Embedding)	*Model-QT(Extraction)*
Mean	2.512195122	2.65365064
Variance	0.807190274	0.868053385
Observations	328	328
df	327	327
F	0.929885521	
P(F<=f) one-tail	0.25568963	
F Critical one-tail	0.833446294	

In the Table 5.7, if F > F Critical one-tail Critical one-tail such that 0.9298 > 0.8334. The variances of the two populations are unequal.

Table 5.8: F-Test for Patt

F-Test Two-Sample for Variances		
	Model-Patt(Extraction)	*Model-Patt(Embedding)*
Mean	11.6697675	8.04011378
Variance	2891.354749	17.87968225
Observations	328	328
df	327	327
F	161.7117524	
P(F<=f) one-tail	6.0355E-266	
F Critical one-tail	1.199837358	

In the Table 5.8, if F > F Critical one-tail Critical one-tail such that 161.7117 > 11998. The variances of the two populations are unequal.

Further, different MIT database images which are high complexity and non-smooth area images other than forest images were investigated to validate the first and second modules developed in the proposed method. The experimental investigation shows the good accuracy level in terms of embedding capacity and imperceptibility. The following Table 5.7 shows the investigation of sample MIT 25 unknown images out of 50 images with respect to proposed module 1 and model based approach. In module 1, the unknown images were experimented with four modified quantization tables with fifteen randomly generated data hiding patterns. The extracted quantization table, data hiding patterns and PSNR values for those images are depicted in the table and the proposed model was investigated by extracting statistical features of DCT elements of those images and the results are laid out in the table. For the selected different sample images displayed in Appendix E, the results of both module 1 and model based approach show the good results and the model is validated for the unknown image set. The remaining 25 images show the unsatisfactory results in terms of model. The results is depicted in the Appendix E. among the 50 MIT unknown image set, the model is working 50% accuracy level.

Table 5.9: Results of model validation for unknown image set

image	QT	Patt	PSNR	Model-QT	Model-Patt
image_0001	2	6	31.3781	2.23E+00	6.01E+00
image_0002	4	12	32.7322	4.12E+00	1.23E+01
image_0003	4	6	37.2819	4.48E+00	5.69E+00
image_0004	3	5	33.16	2.85E+00	5.41E+00
image_0005	2	9	39.3757	1.50E+00	8.88E+00
image_0006	1	4	27.2702	1.23E+00	4.29E+00
image_0007	1	6	32.3241	9.60E-01	5.63E+00
image_0008	2	1	43.5521	2.22E+00	6.50E-01
image_0009	4	12	32.944	4.21E+00	1.23E+01
image_0010	3	4	44.4396	3.31E+00	4.10E+00
image_0011	3	6	30.3437	3.23E+00	6.32E+00
image_0012	3	8	43.3557	3.01E+00	8.02E+00

image_0013	3	3	38.1346	3.01E+00	3.27E+00
image_0014	2	8	33.9175	2.00E+00	8.51E+00
image_0015	2	4	45.2614	1.52E+00	3.54E+00
image_0016	4	4	35.6604	3.91E+00	4.32E+00
image_0017	2	12	32.8886	2.36E+00	1.23E+01
image_0018	2	6	30.6402	2.00E+00	6.25E+00
image_0019	2	6	31.6199	2.01E+00	6.25E+00
image_0020	2	6	35.3922	2.00E+00	6.26E+00
image_0021	4	14	37.3483	4.03E+00	1.39E+01
image_0022	3	6	37.3605	3.25E+00	5.61E+00
image_0023	4	6	41.3858	3.91E+00	6.07E+00
image_0024	3	3	34.0008	3.33E+00	3.50E+00
image_0025	3	15	30.3641	3.61E+00	1.54E+01

5.9. Comparison of the proposed method with recent literature

Paper 1: A Secure Steganography Algorithm Based on Frequency Domain for the transmission of Hidden Information, “Security and Communication Networks” Volume 2017 [115].

Table 5.10: Comparison of proposed method with recent literature

State of the Art	Proposed method
Few JPEG images	JPEG image data set
Entropy thresholding technique	Quantization table modification technique
Public key and private key	Only both are agreed with private keys
Data hiding locations: first seven AC coefficients in the transformed DCT domain	Selected lower frequencies and mid frequencies are utilized
Embedding capacity is low and PSNR is higher than – 45db average	Embedding capacity is very high with acceptable PSNR 30db to 45 dB for image set
Embedding capacity 24bits per block	Embedding capacity > 52 bits/block

Paper 2: Distortion Function for JPEG Steganography Based on Image Texture and Correlation in DCT Domain, “Journal IETE Technical Review”, 2017 [117].

Table 5.11: Comparison of proposed method with recent literature

State of the Art	Proposed method
Distortion function is the key element to select the embedding locations which depends on the magnitude of discrete cosine transformation (DCT) coefficients.	PSNR is the key element to select the data hiding pattern for an image set.
The texture block is identified and used to embed the secrete message based on the amount of zeros in DCT blocks.	DCT contents and quantization table value are used to determine the amount of message to be hidden.
Less detectable artifacts with limited capacity.	High capacity without degrading the image quality.
Boss base image set with quality factor 75.	MIT image set with quality factor 75.

5.10. Chapter Summary

In this chapter, the results of the proposed method are presented and justified with existing standard quantization table modification technique for the selected image set. This section discuss how the selection of fifteen data hiding patterns were derived with existing data hiding pattern by justifying PSNR values and embedding capacity. Then, the selected fifteen data hiding patterns are applied for the selected image set to find the best quantization table and data hiding pattern. The essential parameters of image steganographic techniques such as imperceptibility, embedding capacity, image quality and security are listed and discussed to show the performance of the proposed method by evaluating the relevant quality parameters. Further, the relationship between quantization tables, data hiding patterns and selected image features are derived to generate the identification model that identifies best quantization table and hiding pattern for an image based on the given features.

CHAPTER 6
CONCLUSION AND RECOMENDATIONS

This study investigates the JPEG steganography in terms of quantization table modification. The quantization table modification primarily changes the image features in transform domain and it will affect the imperceptibility and embedding capacity based on the data hiding algorithm. In order to achieve the objectives stated in Chapter 1, the proposed method consists of three stages, modification of primary quantization table for image dataset, data hiding patterns generation in terms of quantization table modification and the generation of dynamic identification model that relates statistical features of DCT coefficients and hiding patterns in favor of quantization table modification. All the three stated stages have been implemented and discussed the merits of the derived results. Following sections elaborate the progress and completion of the research objectives and future research activities.

Improvement of the JPEG image steganography requirements is to increase the embedding capacity without degrading the image quality.

The common primary quantization table used in image dataset is extracted and modified according to literature. Further, the top left part of the modified quantization table is modified by dividing the quantization table values with three threshold values in terms of generating data hiding patterns in lower frequency area. For these modified quantization tables, the newly data hiding patterns are generated by adding more secrete message bits in lower frequencies. Based on the competitive results of PSNR values between the literature and newly generated hiding pattern, fifteen data hiding patterns are generated for the image dataset. Then the fifteen data hiding patterns are the candidate for image dataset with the four quantization tables and it is observed that the minimum PSNR value for the image dataset is 30 and maximum PSNR value for the image dataset is 45. It is the good indicator for the imperceptibility level for the proposed JPEG steganography method that increases the embedding capacity as data hiding happens in middle and lower frequencies. The other quality parameters Normalized cross correlation (NCC) and Structural content (SC) are investigated and they also compete with the results of standard hiding pattern stated in literature. The security of the image steganography is evaluated by the relative entropy based on the probability distribution of image contents and it shows the satisfactory results compared with literature. Further, the file size is investigated after hiding and most of the images in the data set stay with same file size and some of them show the little changes in file size with keeping less distortion. Finally, the proposed system selects the best quantization table for the suitable data hiding pattern in lower frequency with the increase of embedding capacity by minimizing the distortion generated by hiding effect. This proposed system share the pair of selected modified quantization table and generated data hiding patterns as a secrete key with the receiver. The receiver uses the pair to extract the secrete message.

From the results of the proposed system, the proposed module selects the most suitable modified quantization table with relevant data hiding patterns for cover image set based on the assessment of image quality parameters. However, the combination of message size, hiding algorithm and the image contents is the factor to determine the performance of the JPEG steganography method. The consistency of the combination of these factors is kept by generating the dynamic identification model that relates the image contents with the selected quantization table and data hiding pattern. For the selected data hiding patterns in the lower frequency area, the generated dynamic model identifies the modified quantization table and data hiding pattern.

The suggested model based steganography for the selected patterns in terms of quantization table modification hides the secrete message and achieves the perceptual non-detectability with the improved embedding capacity and perceptual quality evaluated by structural similarity. Finally, the generated identification model is stego invariant for message analyzers.

REFERENCES

[1] P. N. Y. B. Babangida Zachariah, "Application of Steganography and Cryptography for Secured Data Communication - A Review," *International Journal of Engineering Research and Technology,* vol. 5, no. 4, pp. 186-190, 2016.

[2] M.Aarti, "Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation," *International Research Journal of Engineering and Technology(IRJET),* vol. 2, no. 1, pp. 397-403, 2015.

[3] M. M. B. C. M. M. a. G. M. S. A. Goel, "A review on data hiding using steganography and visual cryptography," *International Journal of Engineering Development and Research (IJEDR),* vol. 2, 2014.

[4] B. D. S. G.S.Sravanthi, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method," *Global Journal of Computer Science and Technology Graphics & Vision,* vol. 12, no. 15, 2012.

[5] P. Goel, "Data Hiding in Digital Images: A Steganographic paradigm," Indian Institute of Technology Kharagpur, May 2008. [Online]. Available: http://cse. iitkgp.

[6] M. A. B. Y. a. A. Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," *International Journal of Computer Science and Network Security,* vol. 8, no. 6, pp. 247-257, 2008.

[7] R. A. a. C. Z. Wazirali, "The Use of HVS to Estimate Perceptual Threshold for Imperceptible Steganography", *The 30th International conference on Image and Vision Computing (IVCNZ)*," in, New Zealand, 2015.

[8] F. J. L. X. L. a. G. Y. Pan, "Steganography Based On Minimizing Embedding Impact Function and HVS", *International Conference on Electronics, Communications and Control (ICECC)*," in, 2011.

[9] V. H. M. Mansi S. Subhedara, "Current status and key issues in image steganography: A survey," *COMPUTER SCIENCE REVIEW,* 2014.

[10] N. Johnson, "Information Hiding:Steganography and Watermarking-Attacks and Countermeasures," *Advances in Information Security,* 2001.

[11] S. G. K. Mayank Garg, "Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithm", *International Conference on Communication Networks(ICCN)* India, 2015.

[12] P. C. Mandal, "Modern Steganographic techniques:A survey," *International Journal of Computer Science and Engineering Technology(IJCSET),* vol. 3, no. 9, pp. 444-448, 2012.

[13] S. R. P. M. John Babu1, "A Survey on Different Feature Extraction and Classification Techniques Used in Image Steganalysis," *Journal of Information Security,* vol. 8, pp. 186-202, 2017.

[14] K. Rabah, "Steganography-The Art of Hiding Data," *Information Technology Journal ,* vol. 3, pp. 245-269, 2004.

[15] T. G. C.P.Sumathi, "A study of Various Steganographic Techniques used for Information Hiding," *International Journal of Computer Science & Engineering Survey,* vol. 4, no. 6, pp. 9-25, 2013.

[16] M. J. H. Khan Farhan Rafat, "Secure Steganography for Digital Images," *International Journal of Advanced Computer Science and Applications,* vol. 7, no. 6, pp. 45-59, 2016.

[17] B. S. S. S. J. Maninder Sing Rana, "Art of Hiding:An Introduction to Steganography," *International Journal of Engineering And Computer Science,* vol. 1, no. 1, pp. 11-22, 2012.

[18] Q.y. W. J. Z. Xin Liao, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image R.22 (2011) 1–8,* 2011.

[19] Y. L. C. W. I.C. Lin, "Hiding data in spatial domain images with distortion tolerance," *Comput. Stand. Inter. 31 (2),* p. 458–464., 2009.

[20] N. W. C. T. M. H. H.C. Wu, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *Proc. Inst. Elect.Eng., Vis. Images Signal Process 152 (5),* p. 611–615., 2005.

[21] M. M.S.Sutaone, " Image based steganography using LSB insertion technique" *IET International Conference on Wireless,Mobile and Multimedia Networks,*" Beijing,China, 2008.

[22] M. P. S. Aman Arora, " Image steganography using enhanced LSB substitution technique", *Fourth International Conference on Parallel,Distributed and Grid Computing(PDGC),* Waknaghat,India, 2016.

[23] S. K. a. S. Nasr, "New Generating Technique for Image Steganography," *Lecture Notes on Software Engineering,* vol. 1, no. 2, pp. 190-193, 2013.

[24] S. C. Anandaprova Majumder, "I A Novel Approach for Text Steganography :Generating Text Summary using Reflection Symmetry", *International Conference on Computational Intelligence,* India, 2013.

[25] V. D. D. L. Premadasa, T.Kartheeswaran, " Multi teganographyagent based audio steganography", *IEEE International Conference on Computational Intelligence and Computing Research(ICCIC),* India, 2015.

[26] G. R.Balaji, " Secure data transmission using video Steganography", *IEEE International Conference on Electro/Information Technology(EIT),* USA, 2011.

[27] R. G. Sandip Bobade, " Secure Data Communication Using Protocol Steganography*", International Conference on Computing Communication Control and Automation(ICCUBEA),* India, 2015.

[28] J. S. Sumedha Srisikar, " Analysis of Data Hiding Using Digital Image Signal Processing", *International Conference on Electronic Systems,Signal Processing and ComputingTechnologies(ICESC),* Nagpur,India, 2014.

[29] S. A. Priyanka mathur, "data hiding in digital images using steganography paradigm:state of the art," *International Journal of Advances in Electronics and Computer Science,* vol. 4, no. 2, pp. 98-102, 2017.

[30] S. S. Babloo Saha, "Steganographic Techniques of Data Hiding using Digital Images," *Defence Science Journal,* vol. 62, no. 1, pp. 11-18, 2012.

[31] Wei Sun, "High performance reversible data hiding for block truncation coding compressed images," *Signal,Image and Video Processing,* vol. 7, no. 2, pp. 297-306, 2011.

[32] S. B. Sumeet Kaur, "International Conference on Computing for Sustainable Global Development," in *Steganography and classification of image steganography techniques*, India, 2014.

[33] J. Abbas Cheddad, "Digital image steganography:Survey and analysis of current methods," *Signal Processing,* p. 727–752, 2010.

[34] J. H. H. Q. S. Bin Li, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 2, no. 2, pp. 142-171, 2011.

[35] E. B. B. Merrill Warkentin, "Steganography:Forensic,Security,and Legal Issues," *Journal of Digital Forensics, Security and Law,* vol. 3, no. 2, pp. 17-34, 2008.

[36] A. a. H. Zaidoon Kh.AL-Ani, "Overview:Main Fundamentals for Steganography," *JOURNAL OF COMPUTING,* vol. 2, no. 3, pp. 158-165, 2010.

[37] F. M. a. B. Baharudin, "The Statistical Quantized Histogram Texture Features Analysis for Image Retrieval Based on Median and Laplacian Filters in the DCT Domain," *The International Arab Journal of Information Technology,* vol. 10, no. 6, 2013.

[38] W. J. C. C. C. a. L. T. H. N. Chen, "High Payload Steganography Mechanism Using Hybrid Edge," *Expert Systems with Applications* , vol. 37, p. 3292–3301, 2010.

[39] S. A. A. a. P. M. Venkatraman, " Significance of Steganography on Data Security*", The International Conference Information Technology: Coding and Computing*, 2004.

[40] S. W. a. K. S. J. Jung, "A New Histogram Modification Based Reversible Data Hiding Algorithm Considering The Human Visual System," *Signal Processing Letters, IEEE,* vol. 18, no. 2, p. 95–98, 2011.

[41] C. C. L. C. a. W. Y. Chang, "New Image Steganographic Methods Using Run-Length Approach," *Information Sciences,* vol. 176, p. 3393–3408., 2006.

[42] R. Kumar, "HVS Based Steganography," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 2, pp. 43-45, 2013.

[43] Y. h. K. J. L. S. h. a. Q. J. Lu, "An image steganographic method with noise visibility function and dynamic programming strategy on partitioned pixels", *International Conference on Computational Intelligence and Security Workshops, IEEE*, 2007.

[44] T. W.H. Wu, "A Steganographic Method For Images By Pixel Value Differencing," *Pattern Recognition Letters,* vol. 24, p. 1613–1626, 2003.

[45] X. W. Zhang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognition Letters,* vol. 25, no. 3, p. 331–339, 2004.

[46] E. V.M.Potdar, " *Grey level modification steganography for secret communication" ,* 2nd IEEE International Conference on Industrial Informatics," in Berlin,Germany, 2004.

[47] R. jeppiaar, "A Prediction Based Reversible Image Steganographic Algorithm for JPEG Images," *Journal of Applied Security Research,* vol. 10, no. 3, 2015.

[48] S. Hafiz Malik, "IEEE Transactions in Information Forensics and Security," in *Nonparametric Steganalysis of QIM Steganography Using Approximate Entropy*, 2012.

[49] S. A. a. P. Sumari, "An Overview of Frequency-based Digital Image Steganography," *International Journal of Cryptology Research ,* vol. 5, no. 2, pp. 15-27, 2015.

[50] S. N. U. G. R. Barve, "Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform," *International Journal of Computer Science & Communication Networks,* vol. 1, no. 1, pp. 96-99, 2011.

[51] N. K. Manish Mahajan, "Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques," *I. J. Computer Network and Information Security,* vol. 10, pp. 76-92, 2012.

[52] P. T. M. L. C.C. Chang, "An adaptive steganography for index- based images using codeword grouping," *Advances in Multimedia Information Processing-PCM, Springer,* vol. 3333, p. 731–738, 2004.

[53] V. H. Mansi S.Subhedar, "International Conference on Cloud and Ubiquitous Computing & Emerging Technologies," in *Performance Evaluation of Image Steganography based on Cover Selection and Counterlet Transform*, 2013.

[54] M. Y. Q.m. Ying-chun Guo, "No Reference Image Quality Assessment Based on Subbands Similarity and Statistical Analysis for JPEG 2000," *Journal of Electronics and Information Technology,* vol. 33, no. 6, pp. 1496-1500, 2011.

[55] M. L. B. Phi Bang nguyen, "Statistical Analysis of Image Quality metrics for Watermark Transparency Assessment", *Advances in Multimedia Information Processing-PCM* 2010," in, 2010.

[56] A. O. Tunde J.Ogundele, "Evaluation of Multi Level System of Steganography," *International Journal of Information Security Science,* vol. 3, no. 4, pp. 227-231, 2015.

[57] M. K.Rupinder, "A New Efficient Approach towards Steganography," *International Journal of Computer Science and Information Technologies,* vol. 2, no. 2, pp. 673-676, 2011.

[58] G. G. Adel Almohammad, "Stego image quality and the reliability of PSNR*",* *2nd International Conference on Image Processing Theory Tools and Applications(IPTA*)," in, Paris,France, 2010.

[59] S. P. E.P. Musa, "Secret Communication Using Image Steganography," *African Journal of Computing & ICT,* vol. 8, no. 3, 2015.

[60] D. S. K. a. J. D. Neeta, "Implementation of LSB Steganography and Its Evaluation for Various Bits," in *1st International Conference on Digital Information Management(IEEE)*, Bangalore, 2006.

[61] Z. B. N. A. M. H. F. Z. A. Hamdy A. Morsy*, "Information Hiding by Inverting the LSB bits of DCT Coefficients of JPEG images," *Journal of American Science,* vol. 7, no. 11, pp. 171-177, 2011.

[62] R. C. Deepika Bansal, "An Improved DCT based Steganography Technique," *International Journal of Computer Applications,* vol. 102, no. 14, pp. 46-49, 2014.

[63] J. J. Monika Gunjal, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm," *International Journal of Computer Trends and Technology (IJCTT),* vol. 11, no. 4, pp. 144-150, 2014.

[64] S. a. S. Kumar, "Data Hiding in JPEG Images," *International Journal of Information Technology,* vol. 1, no. 1, pp. 13-16, 2009.

[65] C.-C. C. Hsien-Wen Tseng, " Steganography using JPEG-compressed images*",* *The Fourth International Conference onComputer and Information Technology*, Wuhan,China, 2004.

[66] X. L. Y. Y. a. F. L. Yi Zhang, "A frame work of adaptive steganography resisting JPEG compression and detection," *SECURITY AND COMMUNICATION NETWORKS* , vol. 9, pp. 2957-2971, 2016.

[67] F. J. Pevny T, "Multiclass detectorof current steganographic methods for JPEG format," *IEEE Transactions on Information Forensics and Security,* vol. 3, no. 4, pp. 635-650, 2008.

[68] P. J. Ekta Walia, "An Analysis of LSB & DCT based Steganography," *Global Journal of Computer Science and Technology,* vol. 10, no. 1, pp. 4-8, 2010.

[69] H. W. T. a. C. Chang, "Fourth International Conference on Computer and Information Technology," in *Steganography using JPEG- compressed images,* 2004.

[70] H. T. &. C. Chang, "High Capacity Data Hiding in JPEG Compressed Images," *INFORMATICA,* vol. 15, no. 1, pp. 127-142, 2004.

[71] K. M. N. ,. T. B. N. Mahmud Hasan, "A Novel Compressed Domain Technique of Reversible Steganography," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 2, no. 3, 2012.

[72] S. B. D. S. P. S. A. Nag, "A novel technique for image steganography based on Block-DCT and Huffman Encoding," *International Journal of Computer Science and Information Technology,* vol. 2, no. 3, 2010.

[73] P. A. Ajit Danti, "Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography," *IJCA Special Issue on "Recent Trends in Image Processing and Pattern Recognition,* pp. 97-103, 2010.

[74] Z. B. N. A. M. H. a. F. Z. A. Hamdy A. Morsy, "Utilizing Image Block Properties to Embed Data in the DCT Coefficients with Minimum MSE," *International Journal of Computer and Electrical Engineering,* vol. 3, no. 3, pp. 449-453, 2011.

[75] W.-C. C. Po-Yueh Chen, "Secrete Communication Based on Quantization Tables," *International Journal of Applied Science and Engineering,* vol. 13, no. 1, pp. 37-54, 2015.

[76] K. E. A. Chaitanya Kommini, "Image based Secret Communication using Double Compression," *International Journal of Computer Applications,* vol. 21, no. 7, 2011.

[77] R. M. H. G. G. Adel Almohammad, "High Capacity Steganographic Method Based Upon JPEG," *The Third International Conference on Availability, Reliability and Security,* 2008.

[78] N. &. H. P. Provos, "Hide and Seek: An Introduction to Steganography.," *IEEE Security & Privacy Magazine,* vol. 1, pp. 32-44, 2003.

[79] C. L.Z. Chang, "A Steganographic Method Based Upon JPEG and Quantization Table Modification," *Information Sciences,* vol. 141, pp. 123-138, 2002.

[80] N. T.Shohdohji, "Optimization of quantization table based on visual characteristics in DCT image coding," *Computers & Mathematics with Applications,* vol. 37, no. 11-12, pp. 225-232, 1999.

[81] M. S. Yuebing Jiang, " JPEG image compression using quantization table optimization based on perceptual image quality assessment", *Forty Fifth Asilomar Conference on Signals,Systems and Computers*, USA, 2011.

[82] C. a. S. L-W.Chang, "Designing JPEG quantization tables based on human visual system", *International Conference on Image Processing,ICIP 99*," 1999.

[83] K. Gopalan, "International Symbosium on Communications and Information Technologies," in *An image steganography implementation for JPEG - compressed images*, Australiya, 2007.

[84] J. F. TomAs Pevica, " Detection of Double-Compression in JPEG images for Applications in Steganography", *IEEE Transactions on Information Forensics and Security*, 2008.

[85] A. Nidhi Grover, " Digital Image Authentication Model Based on Edge Adaptive Steganography", *2nd International Conference on Advanced Computing,Networking and Security,* India, 2013.

[86] M. Juneja, "A Coveert Communication Model-Bteganographyased on Image Steganography," *International Journal of Information Security and Privacy,* vol. 8, no. 1, p. 19, 2014.

[87] P. Shallee, "Model-based methods for steganography and steganalysis," *International Journal of Image and Graphics,* Vol 5, no. 1, 2005.

[88] M. A. B. Y. a. A. Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion,"*International Journal of Computer Science and Network Security,* vol. 8, 2008.

[89] B. A. a. M. Kaur, "High Capacity Filter Based Steganography," *International Journal of Recent Trends in Engineering,* vol. 1, no. 1, pp. 672-674, 2009.

[90] Y. X. K. X. e. a. Chu R, "A DCT-based image steganographic method resisting statistical attacks", *In Proceedings of (ICASSP '04), IEEE International Conference on Acoustics, Speech and Signal Processing,* 2004.

[91] S. G. &. D. K. Sarmah, "Dynamic Approach of Frequency Based Image Steganography," *International Journal of Applied Engineering Research,* vol. 11, no. 11, pp. 7478-7482, 2016.

[92] S. A. L. a. K. Hemachandran, "Secure data transmission using Steganography and encryption Technique," *International Journal on Cryptography and Information Security,* vol. 3, no. 2, 2012.

[93] T. P. K. Jessica Fridrich, "Proceddings of the 9th workshop on Multimedia & Security," in *Statistically undetectable jpeg steganography:dead ends challanges,and opportunities,* Dallas,Texas,USA, 2007.

[94] R. C. &. A. S. S. Cherukuri, "Switching Theory-Based Steganographic System for JPEG Images," *Mobile Multimedia/Image Processing for Military and Security Applications,* pp. 65790C1-65790C12, 2007.

[95] J. Fridrich, "Proceedings ACM Multimedia and Security Workshop," in *Minimizing the embedding impact in steganography*, Geneva, Switzerland, 2006.

[96] T. P. a. J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis*", Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents*," CA, 2007.

[97] L. F. &. V. A. C. P. Costa, "Identification of the Best Quantization Table Using Genetic Algorithms*", IEEE Pacific Rim Conference on Communications, Computers and signal Processing*,", 2005.

[98] L. Z. Y. N. R. &. Z. Z. Yu, "PM1 steganography in JPEG images using genetic algorithm," *Soft Computing - A Fusion of Foundations, Methodologies and Applications,* vol. 13, pp. 393-400, 2008.

[99] Y.-K. L. a. L.-H. Chen, "Secure Error-Free Steganography for JPEG Images," *International Journal of Pattern Recognition and Artificial Intelligence,* vol. 17, pp. 967-981, 2003.

[100] P. S. B. S. a. G. V. B. Prateek, "A HVS based Perceptual Quality Estimation Measure for Color Images," *ACEEE International Journal on Signal and Image Processing (IJSIP),* vol. 3, no. 1, 2012.

[101] P. A. M. F. &. S. S. H. Watters, "Visual Steganalysis of LSB Encoded Natural Images", *The Third International Conference on Information Technology and Applications*, 2005.

[102] N. Provos, "Defending against statistical steganalysis", *Proceedings of the 10th conference USENIX Security Symposium-Volume 10*, USENIX Association Berkeley, CA, USA, 2001.

[103] P. Westfeld, "High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm)," *Information Hiding. 4th International Workshop. Lecture Notes in Computer Science,* vol. 2137, p. 289– 302, 2001.

[104] I. J. M. M. L. B. J. A. F. J. &. K. T. Cox, Digital Watermarking and Steganography-Second Edition, Burlington, MA, USA: Elsevier Inc, 2008.

[105] P. Sallee, "Model Based Steganography," *The Second International Workshop on Digital Watermarking, IWDW,* pp. 154-167, 2003.

[106] X. &. W. J. Li, "A Steganographic Method Based Upon JPEG and Particle Swarm Optimization Algorithm," *Information Sciences,* vol. 177, pp. 3099-3109, 2007.

[107] A. A. et.al, " JPEG steganography: a performance evaluation of quantization tables", *International Conference on Advanced Information Networking and Applications,* 2009.

[108] Y. P. L. G. B. J. X. G. Cuiling Jiang, "A high capacity steganographic method based on quantization table modification," *Wuhan University Journal of Natural Sciences,* vol. 16, no. 3, p. 223–227, 2011.

[109] D. a. S. V. Brabin, " QET based Steganography Technique for JPEG Images", *International conference on Control, Automation, Communication and Energy conservation*," in, 2009.

[110] Y. P. S. X. Cuiling Jiang, "A High Capacity Steganographic Method Based on Quantization Table Modification and F5 Algorithm," *Circuits, Systems, and Signal Processing,* vol. 33, no. 5, p. 1611–1626, 2014.

[111] K. M. a. A. S. M. Iwata, "Digital Steganography Utilizing Features of JPEG Images," *IEICE Trans. Fundamentals,* Vols. E87-A, no. 4, p. 929–936, 2004.

[112] C. C. L. C. S. T. a. W. L. T. C. C. Chang, "Reversible hiding in DCT-based compressed images," *Information Sciences,* vol. 177, pp. 2768-2786, 2007.

[113] C. C. C. a. Y. Z. W. C. Y. Lin, "Reversible Steganographic Method with High Payload for JPEG Images," *IEICE Trans. Information and Systems,* Vols. 91-D, no. 3, pp. 836-845, 2008.

[114] C. C. L. a. P. F. Shiu, "Proc. of the 3rd International Conference on Ubiquitous Information Management and communication," in *DCT-based reversible data hiding scheme,* 2009.

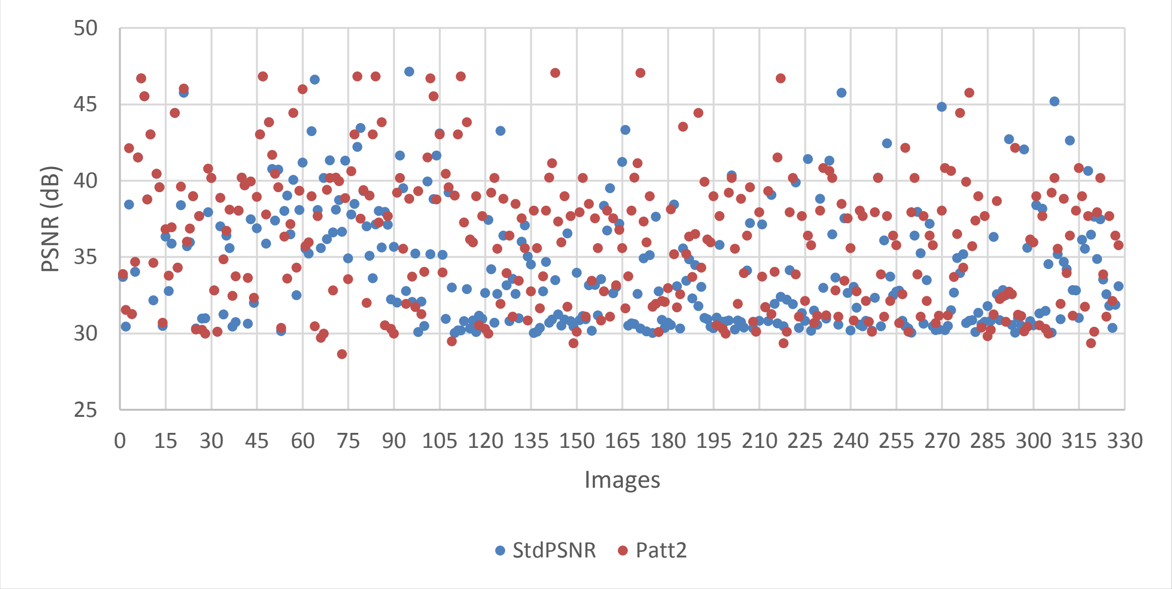
[115] C.-C. C. Hsien-Wen TSENG, "High Capacity Data Hiding in JPEG-Compressed Images," *INFORMATICA, Institute of Mathematics and Informatics, Vilnius,* vol. 15, no. 1, p. 127–142, 2004.

[116] Z.-M. L. Y.-J. H. Kan Wanga, "A high capacity lossless data hiding scheme for JPEG images," *The Journal of Systems and Software,* 2013.

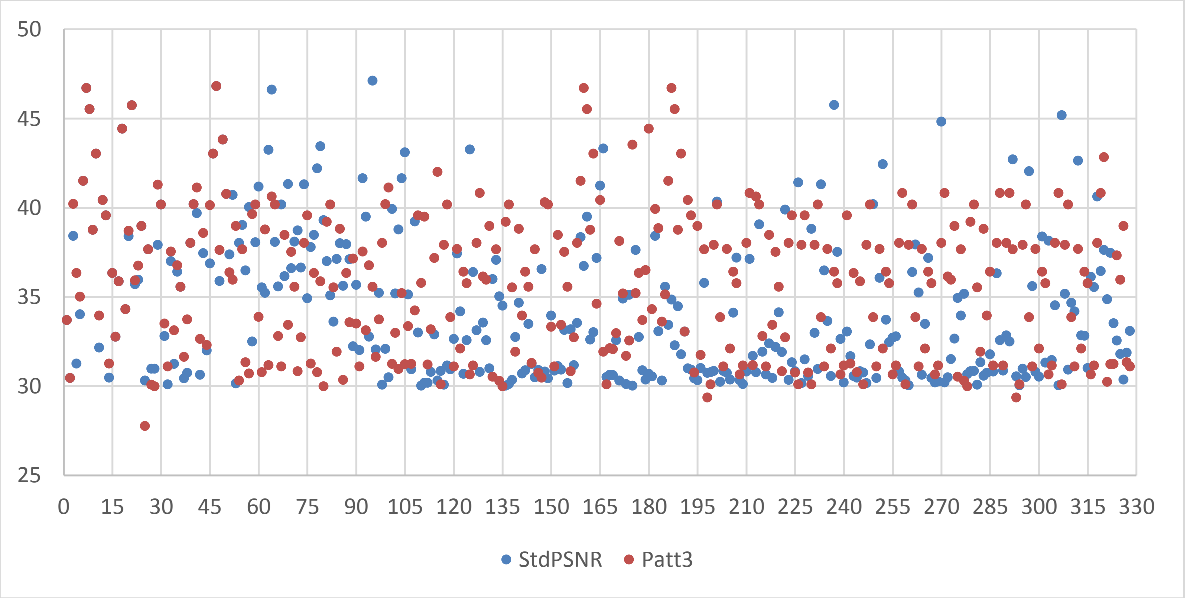
[117] H. M. A. H. M. I. a. A. S. S. Mohamed Amin, "A Steganographic Method Based on DCT and New Quantization Technique," *International Journal of Network Security,* vol. 16, no. 4, pp. 265-270, 2014.

APPENDIX A: COMPARISON OF PSNR VALUES FOR STANDARD HIDING PATTERN AND FIFTEEN GENERATED DATA HIDING PATTERNS

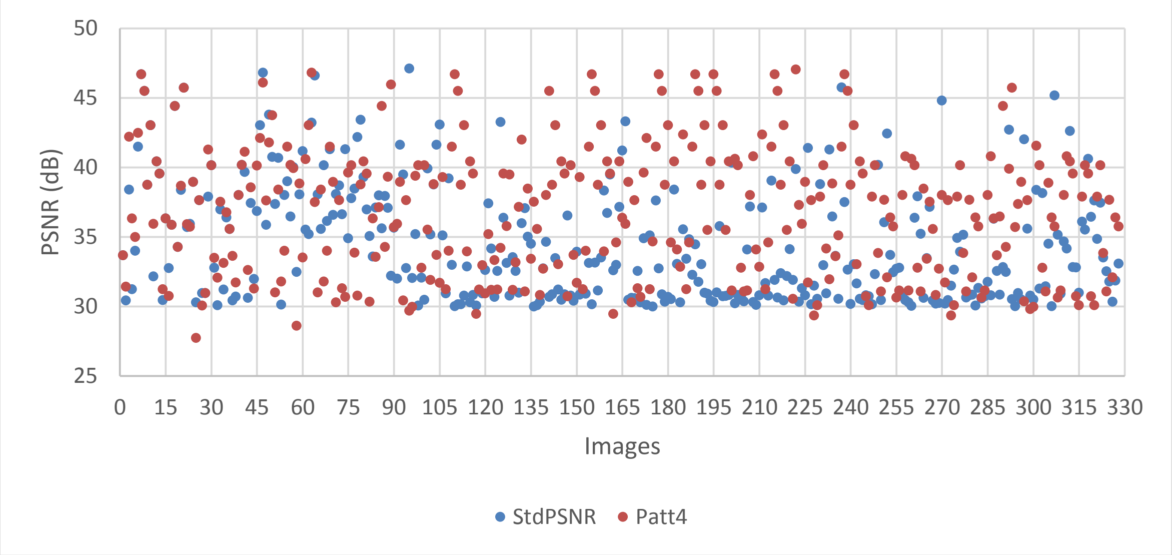
Pattern 2 **vs** StdPSNR



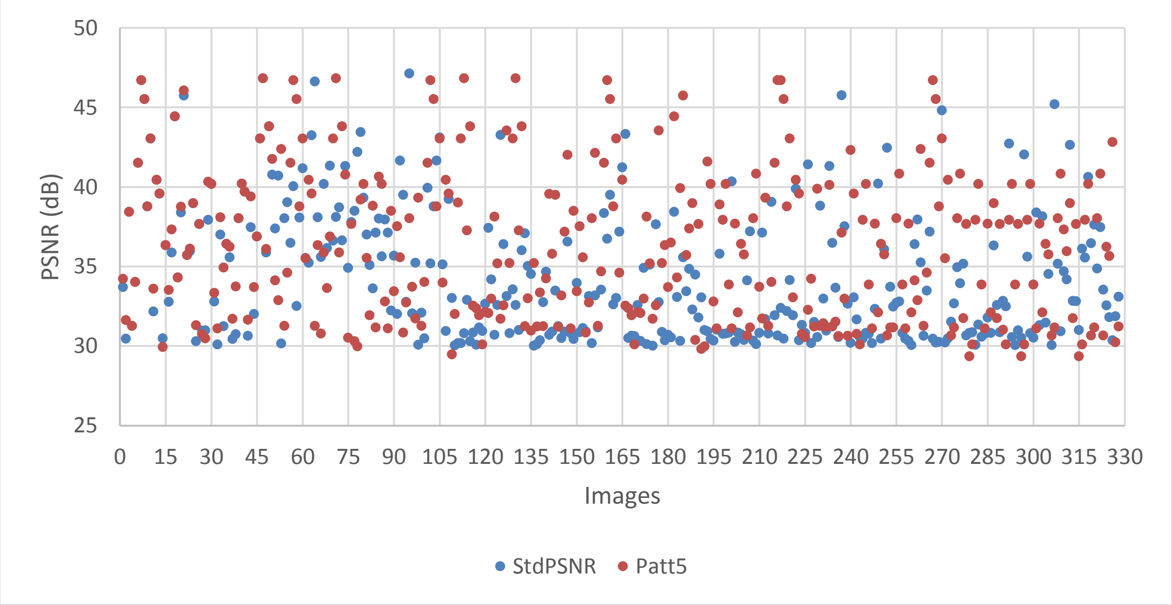
Pattern3 **vs** StdPSNR



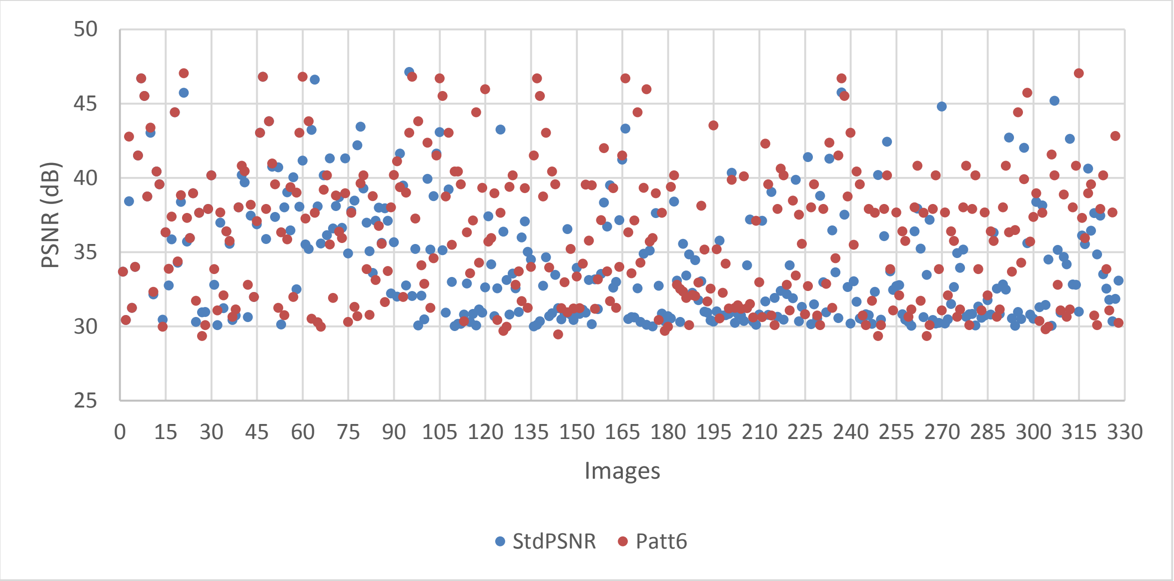
Pattern 4 vs StdPSNR



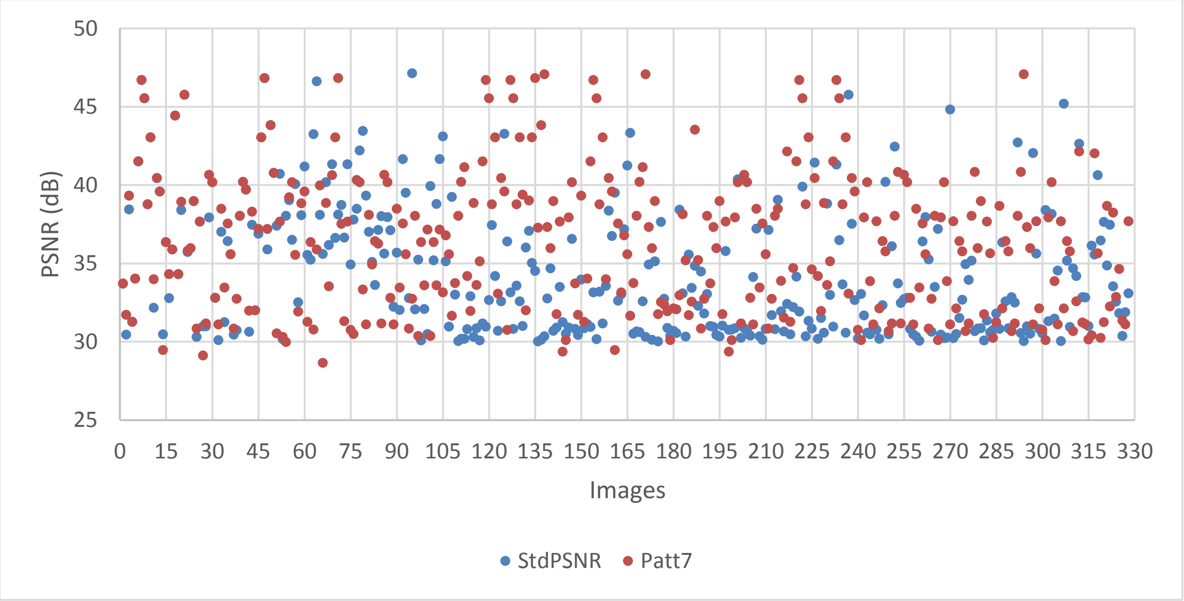
Pattern 5 **vs** StdPSNR



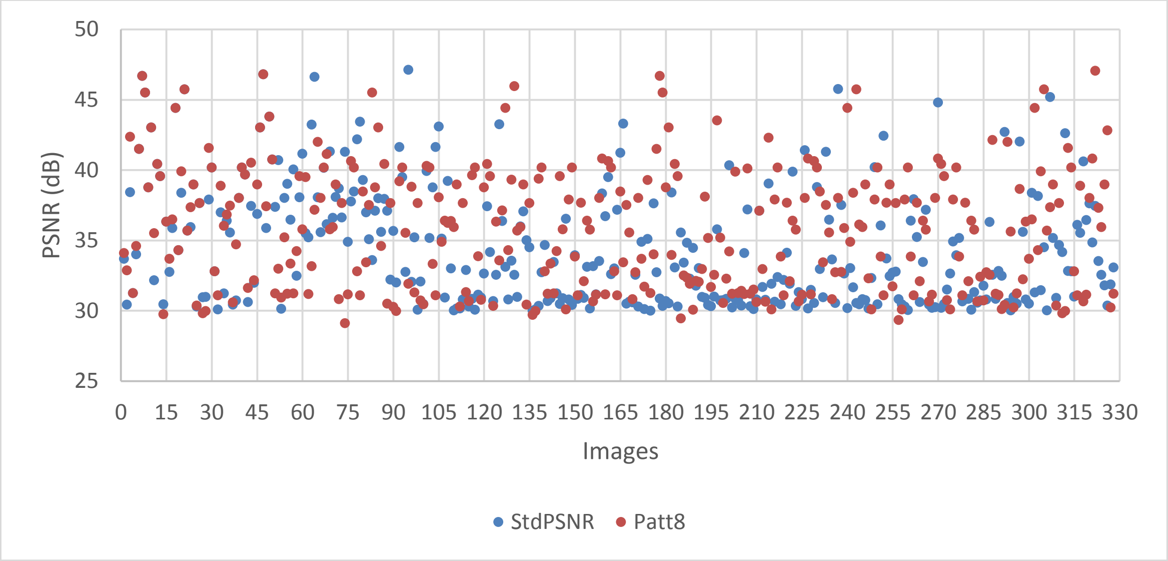
Pattern 6 **vs** StdPSNR



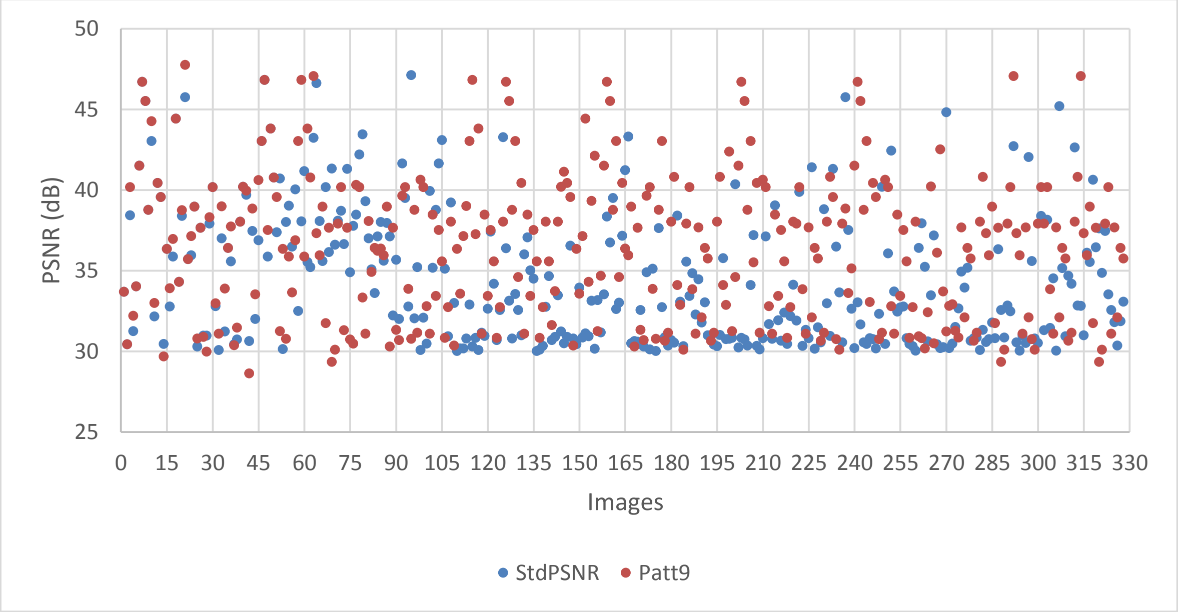
Pattern 7 **vs** StdPSNR



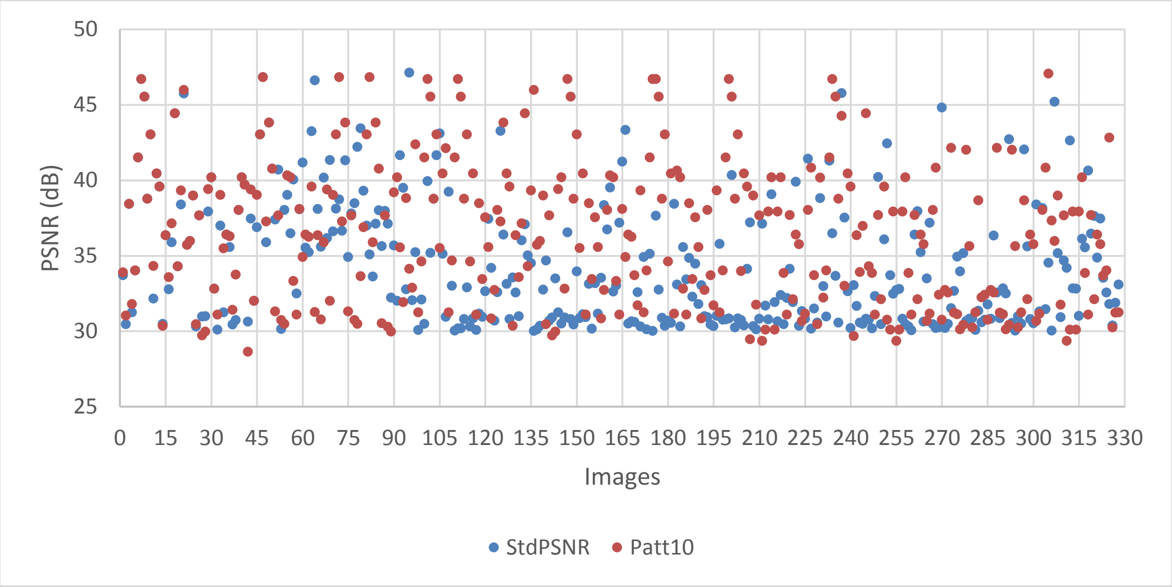
Pattern 8 **vs** StdPSNR



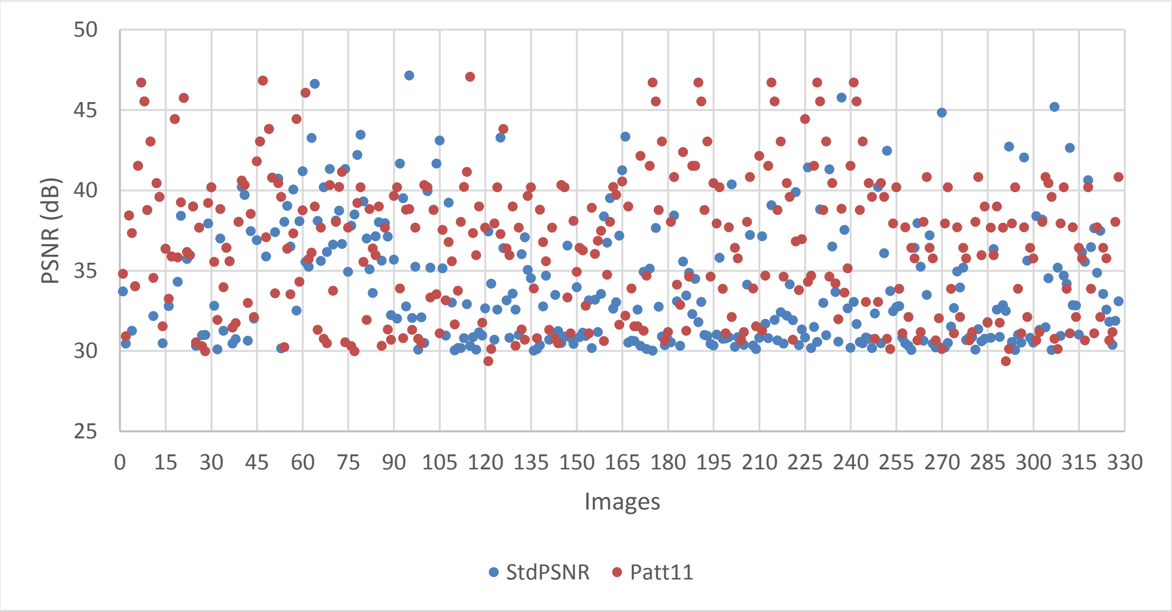
Pattern 9 **vs** StdPSNR



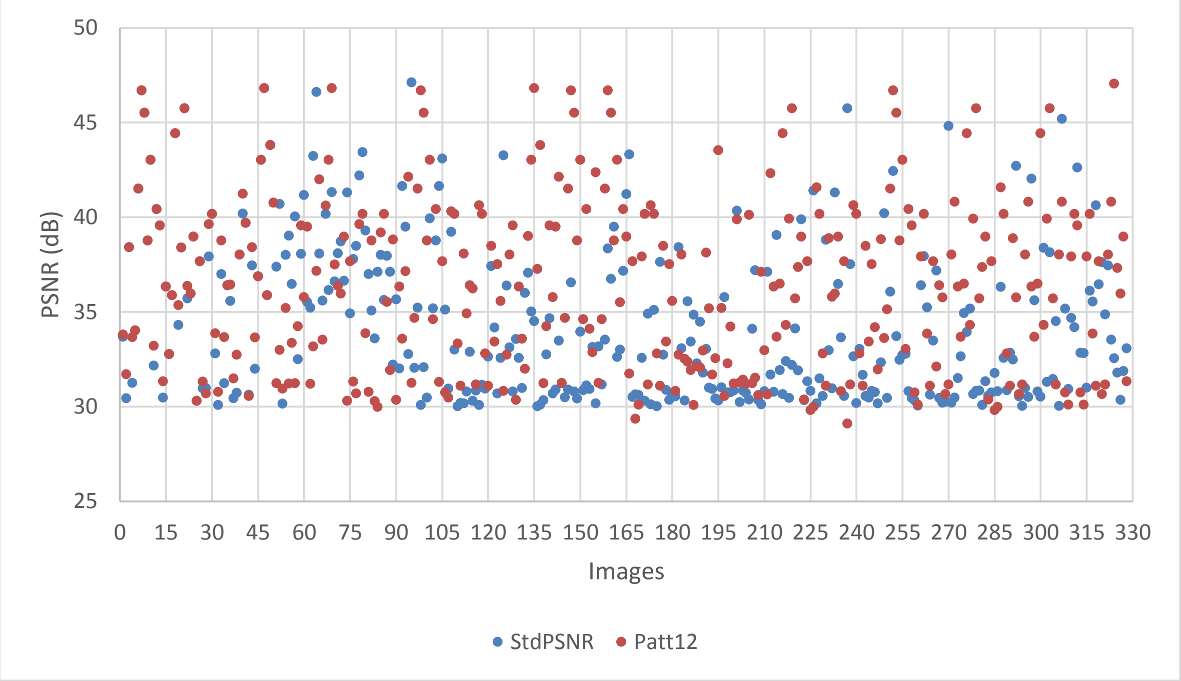
Pattern 10 **vs** StdPSNR



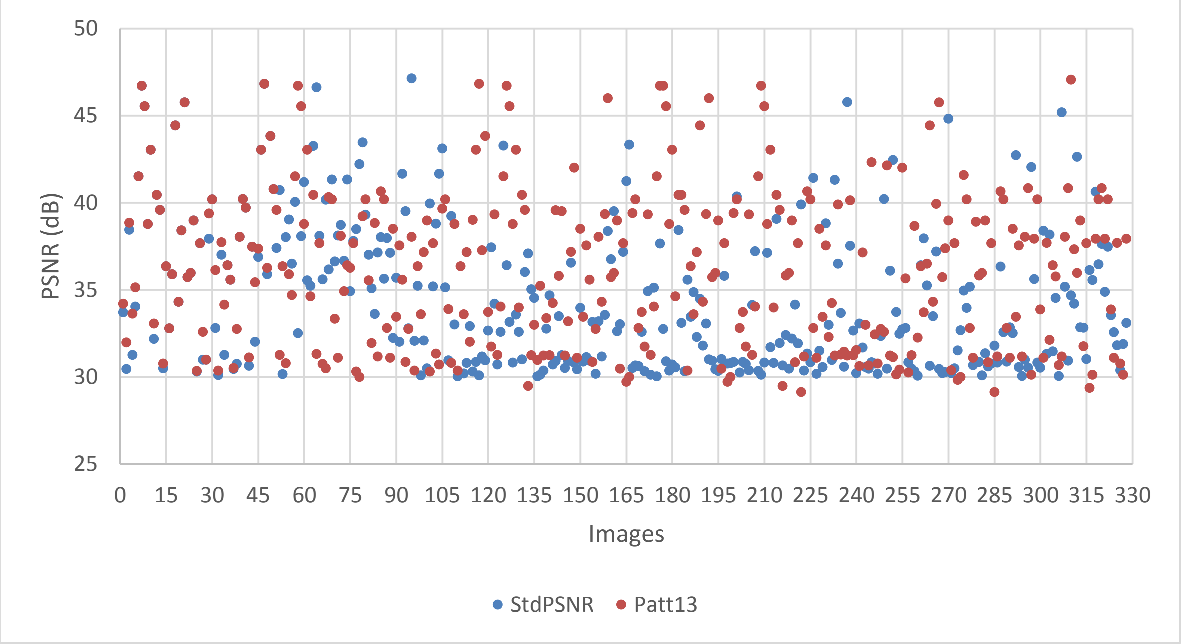
Pattern 11 **vs** StdPSNR



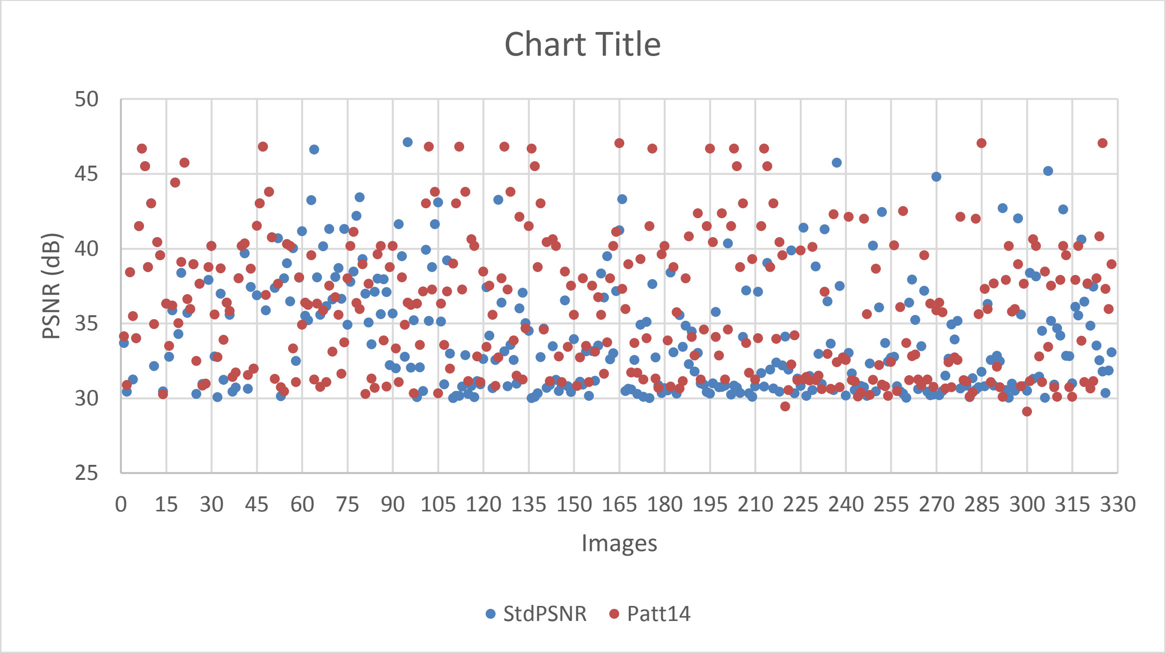
Pattern 12 **vs** StdPSNR



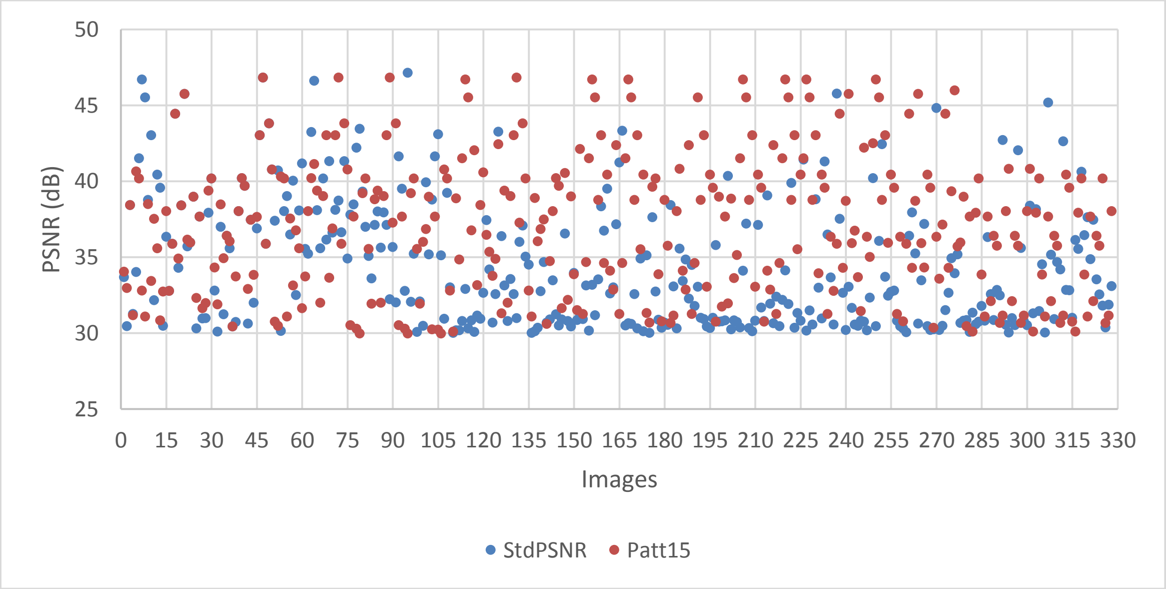
Pattern 13 **vs** StdPSNR



Pattern 14 **vs** StdPSNR

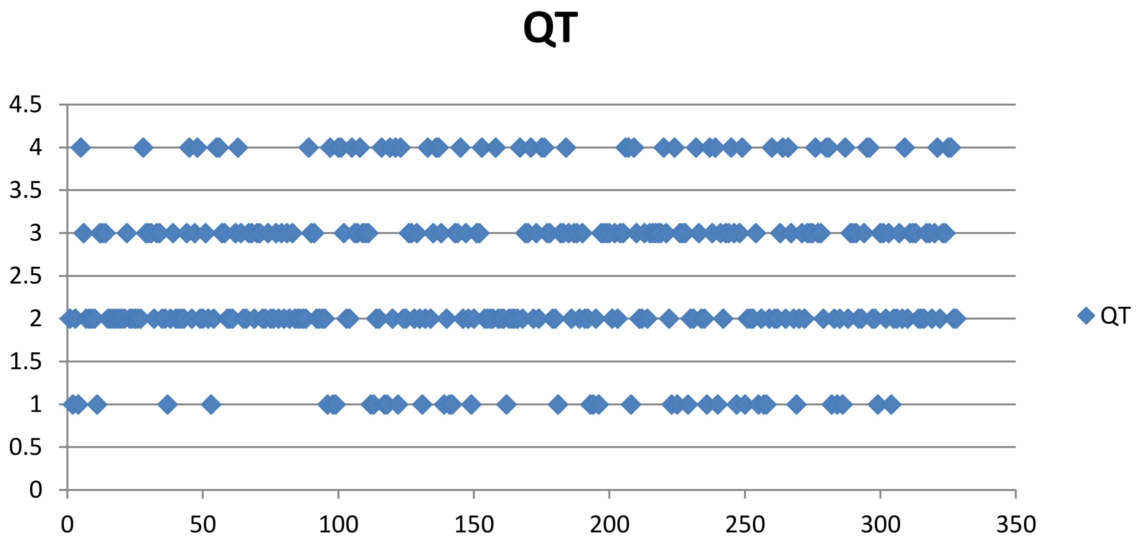


Pattern 15 **vs** StdPSNR

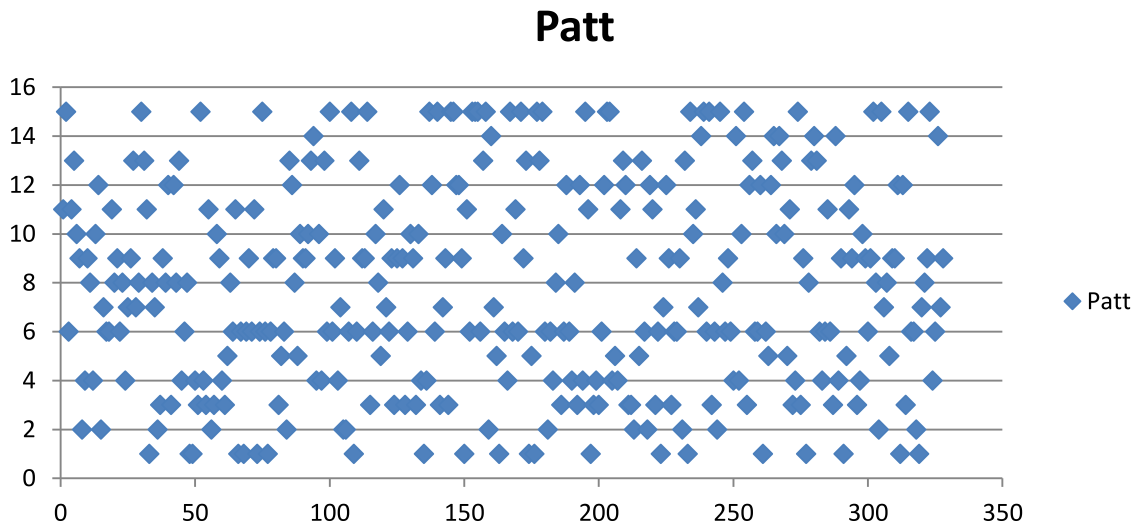


APPENDIX B: RESULTS OF SELECTED QUANTIZATION TABLES AND RELEVANT DATA PATTERNS FOR IMAGE SET

Quantization tables (QT) - **QS$_k$, 1= <k<=4**



Data hiding patterns Patt- **P$_g$, 1=<g<=15**



APPENDIX C: RESULTS OF THE COMPARISON OF VISUAL OBSERVATION OF SAMPLE COVER AND STEGO IMAGES WITH RESPECT TO QUANTIZATION TABLE AND SELECTED DATA HIDING PATTERN

Cover image	Stego Image (QT, P)
 image_0001	 image_0001_Patt_11_Tabel_2
 image_0002	 image_0002_Patt_15_Table_1
 image_0003	 image_0003_Patt_6_Table_2

image_0004	image_0004_Patt_11_Table_1
image_0005	image_0005_Patt_13_Table_4
image_0006	image_0006_Patt_10_Table_3

 image_0007	 image_0007_Patt_9_Table_2
 image_0008	 image_0008_Patt_2_Table_2
 image_0009	 image_0009_Patt_9_Table_2

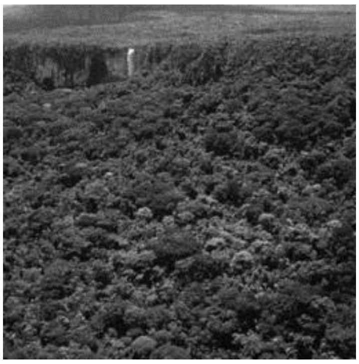
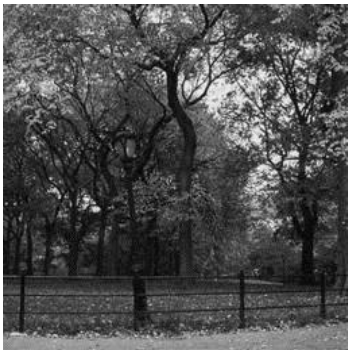
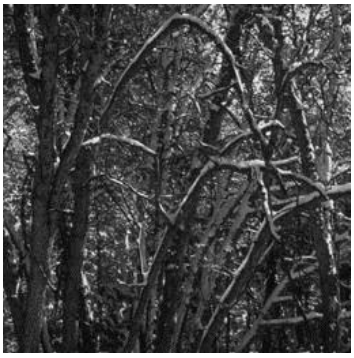
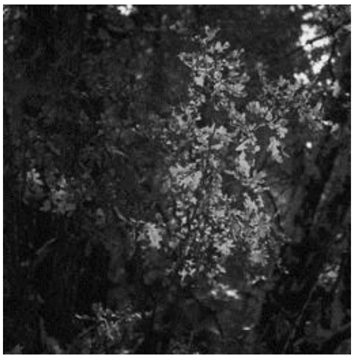
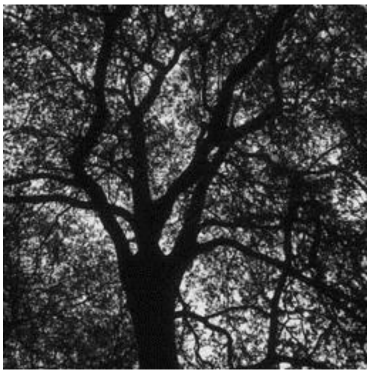
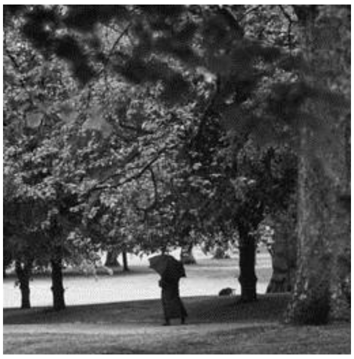
 image_0010	 image_0010_Patt_9_Table_2
 image_0011	 image_0011_Patt_8_Table_1
 image_0012	 image_0012_Patt_4_Table_3

 image_0013	 image_0013_Patt_10_Table_3
 image_0014	 image_0014_Patt_12_Tabel_3
 image_0015	 image_0015_Patt_2_Table_2

APPENDIX D: RESULTS OF STATISTICAL MODLE FOR DIFFERENT COMBINATION OF FEATURE VECTORS

Results 1: Combining the statistical features of DCT elements of cover images with QT using R library

```
> a=lm(QT~X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11 + X12 +
X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20,data=data)

> Summary (a)

Call:

lm(formula = QT ~ X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11 +
X12 + X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20, data = data)

Residuals:

   Min       1Q      Median     3Q       Max

-2.0129  -0.5974   -0.1662    0.5972   1.8388

Coefficients:

            Estimate Std. Error t value Pr(>|t|)

(Intercept)  2.006e+00  2.097e-01   9.566  < 2e-16 ***

X1           5.143e-04  2.089e-04   2.461  0.01411 *

X2          -3.603e-03  7.439e-03  -0.484  0.62834

X3           6.261e-03  8.640e-03   0.725  0.46892

X4          -1.215e-02  1.300e-02  -0.935  0.35027

X5           4.043e-02  2.014e-02   2.008  0.04508 *

X6           1.230e-02  1.085e-02   1.133  0.25775

X7          -1.344e-02  1.598e-02  -0.841  0.40064

X8          -2.043e-02  1.540e-02  -1.326  0.18528

X9          -3.821e-02  1.587e-02  -2.407  0.01636 *

X10         -1.638e-02  1.423e-02  -1.152  0.24989

X11         -9.969e-06  4.642e-04  -0.021  0.98287
```

```
X12          9.342e-03  4.412e-03   2.117  0.03462 *
X13         -1.342e-02  4.835e-03  -2.776  0.00567 **
X14          3.172e-02  1.080e-02   2.938  0.00342 **
X15         -1.633e-02  1.463e-02  -1.116  0.26482
X16         -9.335e-03  9.399e-03  -0.993  0.32098
X17         -5.408e-03  1.010e-02  -0.536  0.59242
X18          3.509e-02  1.702e-02   2.062  0.03958 *
X19         -1.074e-02  1.592e-02  -0.675  0.50021
X20         -1.851e-02  1.108e-02  -1.670  0.09544 .
```

Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.8797 on 635 degrees of freedom

Multiple R-squared: 0.06919,   Adjusted R-squared: 0.03988

F-statistic: 2.36 on 20 and 635 DF, p-value: 0.0007634 – Positive Relationship Model

```
Coefficients:
(Intercept)         X1            X2            X3           X4            X5
  2.006e+00    5.143e-04   -3.603e-03    6.261e-03    -1.215e-02   4.043e-02
        X6            X7            X8            X9           X10           X11
  1.230e-02   -1.344e-02   -2.043e-02    -3.821e-02    -1.638e-02   -9.969e-06
       X12           X13           X14           X15          X16           X17
  9.342e-03   -1.342e-02    3.172e-02   -1.633e-02    -9.335e-03    -5.408e-03
       X18           X19          X20
  3.509e-02   -1.074e-02   -1.851e-02
```

Results 2: Combining the statistical features of DCT elements (DCT-mean, DCT-std) of cover images with data hiding Pattern

```
> a=lm(Patt~X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11 + X12 +
X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20,data=data)

> Summary (a)

Call:

lm(formula = Patt ~ X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 +

    X10 + X11 + X12 + X13 + X14 + X15 + X16 + X17 + X18 + X19 +

    X20, data = data)

Residuals:

   Min     1Q Median     3Q    Max

-9.889 -2.953 -0.007  2.978  9.345

Coefficients:

              Estimate Std. Error t value Pr(>|t|)

(Intercept)  5.8800266  0.9493284   6.194 1.05e-09 ***

X1          -0.0005198  0.0009459  -0.550  0.58284

X2           0.0373551  0.0336732   1.109  0.26770

X3           0.0065309  0.0391119   0.167  0.86744

X4          -0.0095197  0.0588574  -0.162  0.87156

X5           0.0805030  0.0911568   0.883  0.37750

X6          -0.0845951  0.0491370  -1.722  0.08563 .

X7           0.2108195  0.0723567   2.914  0.00370 **

X8          -0.4473427  0.0697228  -6.416 2.74e-10 ***

X9          -0.2342216  0.0718490  -3.260  0.00117 **

X10          0.0263684  0.0643966   0.409  0.68233

X11          0.0020615  0.0021011   0.981  0.32690
```

```
X12          0.0523471  0.0199735   2.621  0.00898 **
X13          0.0172489  0.0218866   0.788  0.43093
X14          0.0136415  0.0488757   0.279  0.78025
X15         -0.1382812  0.0662264  -2.088  0.03720 *
X16         -0.1356348  0.0425461  -3.188  0.00150 **
X17          0.1124124  0.0457064   2.459  0.01418 *
X18          0.1355000  0.0770326   1.759  0.07906 .
X19          0.0296486  0.0720447   0.412  0.68082
X20         -0.0551435  0.0501720  -1.099  0.27215
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
Residual standard error: 3.982 on 635 degrees of freedom
Multiple R-squared:  0.1471,    Adjusted R-squared:  0.1202
F-statistic: 5.476 on 20 and 635 DF,  p-value: 4.598e-13  < 0.05 Positive relationship
```

Model

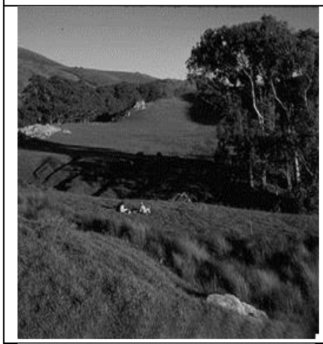
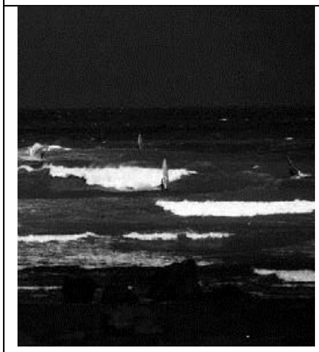
```
Coefficients:
(Intercept)          X1           X2           X3          X4           X5
  5.8800266   -0.0005198   0.0373551   0.0065309   -0.0095197   0.0805030
       X6            X7            X8          X9           X10          X11
-0.0845951    0.2108195    -0.4473427   -0.2342216    0.0263684    0.0020615
      X12           X13           X14          X15           X16          X17
  0.0523471     0.0172489    0.0136415   -0.1382812   -0.1356348    0.1124124
      X18           X19           X20
0.1355000       0.0296486   -0.0551435
```

Correlation

```
> set.seed(100)

> trainingRowIndex <- sample(1:nrow(mydata), 0.8*nrow(mydata))

> trainingData <- mydata[trainingRowIndex, ]

> testData <- mydata[-trainingRowIndex, ]

> lmMod <- lm(Patt ~ X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 + X10 + X11
+ X12 + X13 + X14 + X15 + X16 + X17 + X18 + X19 + X20, data=mydata)

> distPred < predict(lmMod, testData)

Error: object 'distPred' not found

> distPred <- predict(lmMod, testData)

> summary(lmMod)

Call: lm(formula = Patt ~ X1 + X2 + X3 + X4 + X5 + X6 + X7 + X8 + X9 +

    X10 + X11 + X12 + X13 + X14 + X15 + X16 + X17 + X18 + X19 +

    X20, data = mydata)

Residuals:

   Min     1Q Median     3Q    Max

-9.889 -2.953 -0.007  2.978  9.345

Residual standard error: 3.982 on 635 degrees of freedom

Multiple R-squared:  0.1471,    Adjusted R-squared:  0.1202

F-statistic: 5.476 on 20 and 635 DF,  -p-value: 4.598e-13

> actuals_preds <- data.frame(cbind(actuals=testData$Patt, predicteds=distPred))

> correlation_accuracy <- cor(actuals_preds)

71.22%
```

APPENDIX E: SAMPLE UNKNOWN IMAGES FOR MODEL VALIDATION AND

Sample Image set – 25 MIT gray images

Cover Image	Stego-image
	
	

APPENDIX F: UNSATISFACTORY RESULTS OF UNKNOWN IMAGES FOR THE MODEL

image_0026	4	1	29.321	2.21E+00	2.85E+00
image_0027	4	2	31.201	2.10E+00	2.92E+00
image_0028	1	14	30.1	4.23E+00	9.42E+00
image_0029	2	10	30.2301	2.57E+00	8.63E+00
image_0030	2	11	30.4112	2.63E+00	5.79E+00
image_0031	2	10	31.012	5.41E+00	5.23E+00
image_0032	2	5	32.6301	3.12E+00	5.85E+00
image_0033	1	6	29.4521	5.41E+00	1.22E+01
image_0034	3	1	31.561	5.63E+00	1.03E+01
image_0035	4	2	31.23	4.12E+00	3.23E+00
image_0036	1	15	32.005	2.52E+00	1.06E+01
image_0037	1	10	31.203	4.32E+00	1.21E+01
image_0038	3	12	30.1425	4.52E+00	1.02E+01
image_0039	3	3	28.521	3.33E+00	8.42E+00
image_0040	4	6	29.1003	1.06E+00	1.32E+00
image_0041	2	1	29.6301	2.28E+00	1.02E+01
image_0042	3	4	33.3321	4.52E+00	1.11E+01
image_0043	4	8	31.21	1.20E+00	8.12E+00
image_0044	4	7	31.251	4.56E+00	7.85E+00
image_0045	1	2	30.0623	2.59E+00	5.40E+00
image_0046	1	6	30.2561	4.21E+00	6.24E+00
image_0047	1	6	32.0471	5.28E+00	6.21E+00
image_0048	2	3	31.85	2.82E+00	3.75E+00
image_0049	3	2	29.0054	1.41E+00	1.13E+00
image_0050	1	7	31.23	1.76E+00	4.18E+00

APPENDIX G: PUBLICATIONS BASED ON THIS RESEARCH STUDY

Peer Reviewed Journal Article

V.Senthooran, L.Ranathunga, "An Experimental Investigation of Statistical Model based Secure Steganography for JPEG images", Indian Journal of Science and Technology, *Vol 10(2017), DOI:10.17485/IJST/2017/V10i27/111440,July 2017*.

IEEE Indexed Conference Publications

V.Senthooran, L.Ranathunga, "DCT coefficient dependent quantization table modification steganographic algorithm, First International Conference on Networks & Soft Computing (ICNSC), 2014, pp. 432–436.

V.Senthooran, L.Ranathunga, "An investigation of quantization table modification table on JPEG steganography, 8th IEEE International Conference on Industrial and Information Systems (ICIIS), pp.2014, 622-626